

# OLITEC

# ADSL Wi-Fi SG

# 108 Mbps

## *RW400SG Router OLITEC*

### User's Guide





Chapter 1: Introduction.....	1
2.1 Overview of the Router .....	1
2.2 Features.....	1
2.3 Panel Layout.....	2
2.3.1 The Front Panel .....	2
2.3.2 The Rear Panel.....	3
Chapter 3: Connecting the Router .....	4
3.1 System Requirements.....	4
3.2 Installation Environment Requirements.....	4
3.3 Connecting the Router .....	4
Chapter 4: Quick Installation Guide.....	6
4.1 TCP/IP configuration .....	6
4.2 Quick Installation Guide .....	7
Chapter 5: Configuring the Router .....	11
5.1 login .....	11
5.2 Status.....	11
5.3 Quick Setup .....	12
5.4 Network.....	12
5.4.1 LAN.....	13
5.4.2 WAN.....	13
5.4.3 MAC Clone .....	18
5.5 Wireless .....	19
5.5.1 Wireless Settings .....	19
5.5.2 MAC Filtering .....	22
5.5.3 Wireless Statistics .....	24
5.6 DHCP.....	25
5.6.1 DHCP Settings.....	25
5.6.2 DHCP Clients List .....	26
5.6.3 Address Reservation.....	27
5.7 Forwarding .....	28
5.7.1 Virtual Servers .....	28
5.7.2 Port Triggering .....	29
5.7.3 DMZ.....	31
5.7.4 UPnP .....	32
5.8 Security .....	33
5.8.1 Firewall .....	33
5.8.2 IP Address Filtering.....	34
5.8.3 Domain Filtering.....	35
5.8.4 MAC Filtering .....	37
5.8.5 Remote Management .....	38
5.8.6 Advanced Security .....	39
5.9 Static Routing.....	41
5.10 DDNS.....	42
5.10.1 Dyn dns.org DDNS .....	42

5.10.2 Oray.net DDNS .....	42
5.10.3 Comexe.cn DDNS.....	43
5.11 System Tools .....	44
5.11.1 Time .....	45
5.11.2 Firmware .....	45
5.11.3 Factory Defaults .....	46
5.11.4 Reboot .....	46
5.11.5 Password .....	47
5.11.6 Log .....	48
5.11.7 Statistics .....	48
Appendix A: FAQ.....	50
Appendix B: Configuring the PCs.....	54
Appendix C: Specifications.....	59
Appendix D: Glossary .....	60
Appendix E: Contact Information.....	<b>Erreur ! Signet non défini.</b>

## Chapter 2: Introduction

### 2.1 Overview of the Router

The RW400SG 108Mbps Wireless Router integrates 4-port Switch, firewall, NAT-router and Wireless AP. Its design is dedicated to Small Office/Home Office (SOHO) wireless network solutions. The RW400SG 108Mbps Wireless Router will allow you to connect your network wirelessly better than ever, sharing Internet Access, files and fun, easily and securely.

In the most attentive wireless security, the RW400SG 108Mbps Wireless Router provides multiple protection measures. It can be set to turn off wireless network name (SSID) broadcast so that only stations that have the SSID can be connected. The router provides wireless LAN 64/128/152-bit WEP encryption security, and WPA/WPA2 and WPA-PSK/WPA2-PSK authentication, as well as TKIP/AES encryption security. It also supports VPN pass-through for sensitive data secure transmission.

The RW400SG 108Mbps Wireless Router complies with the IEEE 802.11g/b standards and adopts **108M Super G™ WLAN transmission technology** so that the data transmission rate is up to 108Mbps. It adopts **2x to 3x eXtended Range™ WLAN transmission technology** so that transmission distance is 2-3 times of traditional IEEE 802.11g/b solutions, up to a distance of 855.36m tested in China. Transmission range is extended to 4-9 times. It is compatible with all IEEE 802.11g and IEEE 802.11b products.

The RW400SG 108Mbps Wireless Router provides flexible access control so that parents or network administrators can establish restricted access policies for children or staff. It has built-in NAT and DHCP server supporting static IP address distributing. It also supports Virtual Server and DMZ host for Port Triggering needs, and remote management and log so that network administrators can manage and monitor the network on real time.

The RW400SG 108Mbps Wireless Router is easy-to-manage. Quick Setup is supported and friendly help messages are provided for every step. So you can configure it quickly and share Internet access, files and fun.

### 2.2 Features

- Complies with IEEE802.11g, IEEE802.11b, IEEE802.3, IEEE802.3u standards
- Built in 4-port 10/100Mbps Switch
- Ethernet connection to a WAN device, such as a cable modem or DSL modem
- Adopts **108M Super G™ and 2x to 3x eXtended Range™** WLAN transmission technologies
- Shares data and Internet access for the network, connecting Internet through PPPoE on demand and disconnecting when idle
- Supports 108/54/48/36/24/18/12/9/6Mbps or 11/5.5/3/2/1Mbps wireless LAN data transfer rates
- Provides 64/128/152-bit WEP encryption security
- Provides WPA/WPA2 and WPA-PSK/WPA2-PSK authentication and TKIP/AES encryption security

- Provides wireless LAN ACL (Access Control List)
- Built-in NAT and DHCP server supporting static IP address distributing
- Supports Virtual Server, Port Triggering, and DMZ host
- Built-in firewall supporting IP address filtering, Domain Name filtering, and MAC address filtering
- Supports connecting/disconnecting Internet at a specified time of day
- Supports access control, allowing parents and network administrators to establish restricted access policies based on the time of day for children or staff
- Supports TCP/IP, PPPoE, DHCP, ICMP, NAT, SNTP
- Supports UPnP, Dynamic DNS, Static Routing, VPN pass-through
- Supports Traffic Statistics
- Supports ICMP-FLOOD, UDP-FLOOD, TCP-SYN-FLOOD filter
- Ignores Ping packets from WAN or LAN ports
- Supports firmware upgrade
- Supports Remote and Web management

## 2.3 Panel Layout

### 2.3.1 The Front Panel

The front panel of the RW400SG consists of several LED indicators, which is designed to indicate connections. Viewed from left to right. Table 2-1 describes the LEDs on the front panel of the router.



Figure 2-1: Front Panel sketch

Name	Action	Description
Power	Not lit	No Power
	Lit up	Power on
STATUS	Lit up	The router is initialising
	Flashing	The router is working properly
	Not lit	The router has a hardware error
WAN/LAN	Not lit	There is no device linked to the corresponding port
	Lit up	There is a device linked to the corresponding port but no activity
	Flashing	There is an active device linked to the corresponding port
WLAN	Not lit	The Wireless Radio function is disabled
	Flashing	The Wireless Radio function is enabled

Table 2-1 The LEDs description

### 2.3.2 The Rear Panel

The rear panel contains the following features. (Viewed from left to right:)

- Wireless antenna
  - Factory Default Reset button
  - There are two ways to reset the router's factory defaults:
    - 1) Use the **Factory Defaults** function on **System Tools** -> **Factory Defaults** page in the router's Web-based Utility.
    - 2) Use the Factory Default Reset button: First, turn off the router's power. Second, press and hold the default reset button then turn on the router's power, until the system LED lights up (about 3 seconds). Last, release the reset button and wait for the router to reboot.
- Note:** Ensure the router is powered on before it restarts completely.
- WAN RJ45 port for connecting the router to a cable, DSL modem, or Ethernet
  - Four LAN 10/100Mbps RJ45 ports for connecting the router to the local PCs
  - AC power socket: only use the power adapter supplied with the RW400SG 108Mbps Wireless Router, use of a different adapter may result in product damage.

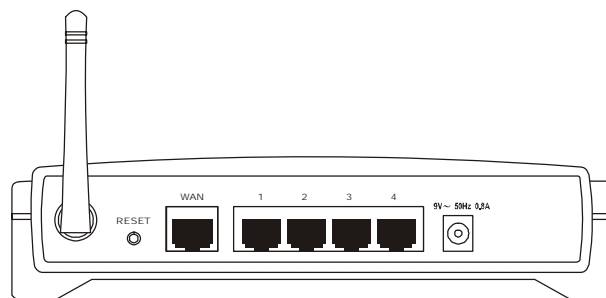


Figure 2-2: Rear Panel sketch

## Chapter 3: Connecting the Router

### 3.1 System Requirements

- Broadband Internet Access Service (DSL/Cable/Ethernet)
- One DSL/Cable modem that has an RJ45 connector (you do not need it if you connect the router to Ethernet)
- Each PC on the LAN needs a working Ethernet Adapter and an Ethernet cable with RJ45 connectors
- TCP/IP protocol must be installed on each PC
- Web browser, such as Microsoft Internet Explorer 5.0 or later, Netscape Navigator 6.0 or later

### 3.2 Installation Environment Requirements

- Not in direct sunlight or near a heater or heating vent
- Not cluttered or crowded. There should be at least 2 inches (5 cm) of clear space on all sides of the router
- Well ventilated (especially if it is in a closet)
- Operating temperature: 0°C~40°C (32°F~104°F)
- Operating Humidity: 10%~90%RH, Non-condensing

### 3.3 Connecting the Router

Before you install the router, you should connect your PC to the Internet through your broadband service successfully. If there is any problem, please contact your ISP. After that, please install the router according to the following steps. Don't forget to pull out the power plug and keep your hands dry.

1. Power off your PC(s), Cable/DSL modem, and the router.
2. Locate an optimum location for the router. The best place is usually near the center of the area in which your PC(s) will wirelessly connect. The place must accord with the [Installation Environment Requirements](#).
3. Adjust the direction of the antenna. Normally, upright is a good direction.
4. Connect the PC(s) and each Switch/Hub on your LAN to the LAN Ports on the router, shown in figure 3-1.
5. Connect the DSL/Cable Modem to the WAN port on the router, shown in figure 3-1.
6. Connect the AC power adapter to the AC power socket on the router, and the other end into an electrical outlet. The router will start to work automatically.
7. Power on your PC(s) and Cable/DSL modem.



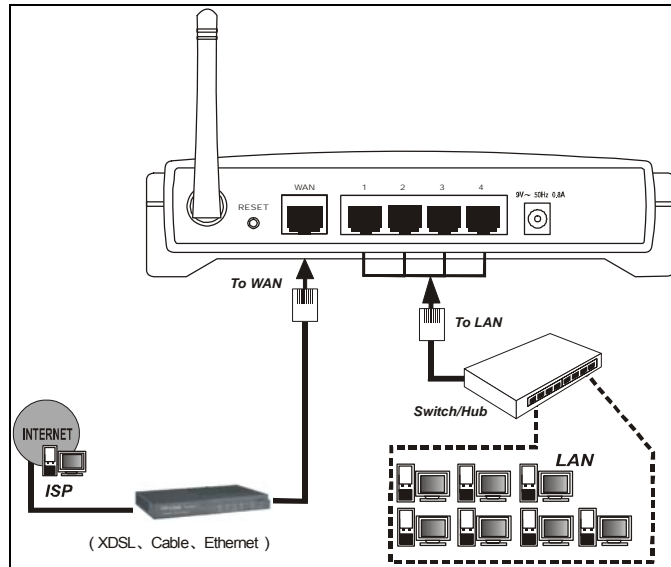


Figure 3-1: Hardware Installation of the RW400SG 108Mbps Wireless Router

## Chapter 4: Quick Installation Guide

After connecting the RW400SG Router into your network, you should configure it. This chapter describes how to configure the basic functions of your RW400SG Wireless Router. These procedures only take you a few minutes. You can access the Internet via the router immediately after successfully configured.

### 4.1 TCP/IP configuration

The default IP address of the RW400SG 108Mbps Wireless Router is 192.168.1.1, and the default Subnet Mask is 255.255.255.0. These values can be seen from the LAN. They can be changed as you desire, as an example we use the default values for description in this guide.

Connect the local PCs to the LAN ports on the router. There are then two means to configure the IP address for your PCs.

- Configure the IP address manually
  - 1) Set up the TCP/IP Protocol for your PC(s). If you need instructions as to how to do this, please refer to [Appendix B: "Configuring the PCs."](#)
  - 2) Configure the network parameters. The IP address is 192.168.1.xxx ("xxx" is from 2 to 254), Subnet Mask is 255.255.255.0, and Gateway is 192.168.1.1 (The router's default IP address)
- Obtain an IP address automatically
  - 1) Set up the TCP/IP Protocol in "**Obtain an IP address automatically**" mode on your PC(s). If you need instructions as to how to do this, please refer to [Appendix B: "Configuring the PCs."](#)
  - 2) Power off the router and PC(s). Then turn on the router, and restart the PC(s). The built-in DHCP server will assign IP addresses for the PC(s).

Now, you can run the Ping command in the **command prompt** to verify the network connection between your PC(s) and the router. The following example is in Windows 2000 OS.

Open a command prompt, and type *ping 192.168.1.1*, then press **Enter**.

```
Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<10ms TTL=64
Reply from 192.168.1.1: bytes=32 time<10ms TTL=64
Reply from 192.168.1.1: bytes=32 time<10ms TTL=64
Reply from 192.168.1.1: bytes=32 time<10ms TTL=64

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Figure 4-1: Successful result of Ping command

If the result displayed is similar to that shown in figure 4-1, the connection between your PC and the router has been established.

```
Pinging 192.168.1.1 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Figure 4-2: Failed result of Ping command

If the result displayed is similar to that shown in figure 4-2, it means that your PC has not connected to the router. Please check it following these steps:

1. Is the connection between your PC and the router correct?  
**Note:** The Link/Act LEDs of LAN port on the router and LEDs on your PC's adapter should be lit.
2. Is the TCP/IP configuration for your PC correct?  
**Note:** If the router's IP address is 192.168.1.1, your PC's IP address must be within the range of 192.168.1.2 ~ 192.168.1.254, the gateway must be 192.168.1.1

## 4.2 Quick Installation Guide

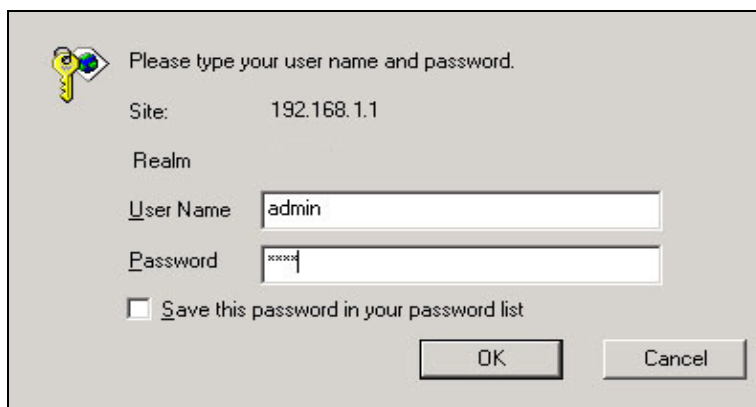
With a Web-based (Internet Explorer or Netscape® Navigator) utility, the TL-WR541G 54Mbps Wireless Router is easy to configure and manage. The Web-based utility can be used on any Windows, Macintosh or UNIX OS with a web browser.

Connect to the router by typing `http://192.168.1.1` in the address field of web browser.



Figure 4-3 Login to the router

After a moment, a login window will appear similar to that shown in Figure 4-4. Enter **admin** for the User Name and Password, both in lower case letters. Then click the **OK** button or press the **Enter** key.



Please type your user name and password.

Site: 192.168.1.1

Realm

User Name: admin

Password: [masked]

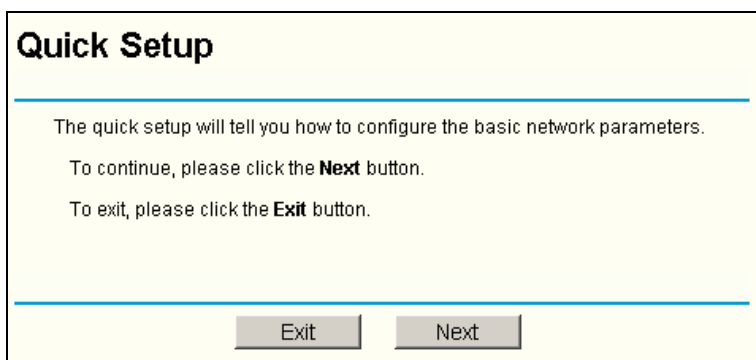
☐ Save this password in your password list

OK Cancel

Figure 4-4 Login Windows

**Note:** If the above screen does not prompt, it means that your web-browser has been set to a proxy. Go to Tools menu>Internet Options>Connections>LAN Settings, in the screen that appears, cancel the Using Proxy checkbox, and click OK to finish it.

If the User Name and Password are correct, you can configure the router using the web browser. Please click the **Quick Setup** link on the left of the main menu and the Quick Setup screen will appear.



### Quick Setup

The quick setup will tell you how to configure the basic network parameters.

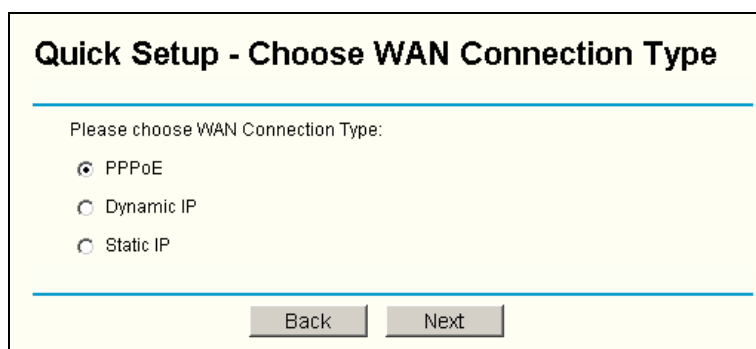
To continue, please click the **Next** button.

To exit, please click the **Exit** button.

Exit Next

Figure 4-5 Quick Setup

Click **Next**, the **Choose WAN Connection Type** page will appear, shown in figure 4-6.



### Quick Setup - Choose WAN Connection Type

Please choose WAN Connection Type:

- ☒ PPPoE
- ☐ Dynamic IP
- ☐ Static IP

Back Next

Figure 4-6 Choose WAN Connection Type

The router supports three popular ways to connect to Internet. Please select one compatible with your ISP. Click **Next** to enter the necessary network parameters.

If you choose "**PPPoE**", you will see this page shown in figure 4-7:

Figure 4-7 Quick Setup - PPPoE

- **User Name and Password** - Enter the **User Name** and **Password** provided by your ISP. These fields are case sensitive. If you have difficulty with this process, please contact your ISP.

If you choose "**Dynamic IP**", the router will automatically receive the IP parameters from your ISP without needing to enter any parameters.

If you Choose "**Static IP**", the Static IP settings page will appear, shown in figure 4-8:

Figure 4-8 Quick Setup - Static IP

**Note:** The IP parameters should have been provided by your ISP.

- **IP Address** - This is the WAN IP address as seen by external users on the Internet (including your ISP). Enter the IP address into the field.
- **Subnet Mask** - The Subnet Mask is used for the WAN IP address, it is usually 255.255.255.0
- **Default Gateway** - Enter the gateway into the box if required.
- **Primary DNS** - Enter the DNS Server IP address into the boxes if required.
- **Secondary DNS** - If your ISP provides another DNS server, enter it into this field.

After you complete the above, click **Next**, the Wireless settings page will appear, shown in figure 4-9.

Figure 4-9 Quick Setup - Wireless settings

In this page, you can configure the following wireless parameters:

- **Wireless Radio** - indicates whether the Access Point feature of the router is enabled or disabled. If disabled, the WLAN LED on the front panel will not be lit and the wireless stations will not be able to access the router. If enabled, the WLAN LED will be lit up and wireless stations will be able to access the router.
- **SSID** - Enter a value of up to 32 characters. The same SSID must be assigned to all wireless devices on your network. The default SSID is default. This value is case-sensitive. For example, *default* is NOT the same as *DEFAULT*.
- **Region** - Select your region from the pull-down list. This field specifies the region where the wireless function of the router can be used. It may be illegal to use the wireless function of the router in a region other than one of those specified in this field.
- **Channel** - the current channel in use. This field determines which operating frequency will be used.
- **Mode** - Indicates the current mode (**108Mbps (Dynamic)**, **108Mbps (Static)**, **54Mbps (802.11g)**, **11Mbps (802.11b)**). If you select **108Mbps (Dynamic)**, it is compatible with **54Mbps (802.11g)** and **11Mbps (802.11b)**. If you select **54Mbps (802.11g)**, it is compatible with **11Mbps (802.11b)**.

These settings are only for basic wireless parameters, for advanced settings, please refer to [Section 5.5: "Wireless."](#)

**Note:** The change of wireless settings won't take effect until the router reboots! You can reboot it manually. If you need instructions as to how to do this, please refer to [Section 5.11.4: "Rebooting the Router"](#)

Click the **Next** button, you will then see the Finish page:

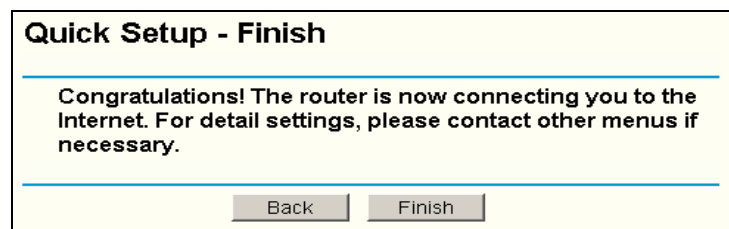


Figure 4-10 Quick Setup - Finish

After finishing all configurations of basic network parameters, please click **Finish** button to exit this **Quick Setup**.

## Chapter 5: Configuring the Router

This chapter describes each web page's key functions.

### 5.1 login

After your successful login, you can configure and manage the router. There are ten main menus on the left of the web-based utility. Submenus will be available after you click one of the main menus. The ten main menus are: **Status, Quick Setup, Network, Wireless, DHCP, Forwarding, Security, Static Routing, DDNS and System Tools**. On the right of the web-based utility, there are the detailed explanations and instructions for the corresponding page. To apply any settings you have altered on the page, please click the **Save** button.

There are the detailed explanations for each web page's key functions below.

### 5.2 Status

The Status page displays the router's current status and configuration. All information is read-only.

#### 1. LAN

This field displays the current settings or information for the LAN, including the **MAC address, IP address and Subnet Mask**.

#### 2. Wireless

This field displays basic information or status for wireless function, including **Wireless Radio, SSID, Channel, Mode, Wireless MAC address and IP address**.

#### 3. WAN

These parameters apply to the WAN port of the router, including **MAC address, IP address, Subnet Mask, Default Gateway, DNS server and WAN connection type**. If PPPoE is chosen as the WAN connection type, the **Disconnect** button will be shown here while you are accessing the Internet. You can also cut the connection by clicking the button. If you have not connected to the Internet, a **Connect** button will be shown, you can then establish the connection by clicking the button.

#### 4. Traffic Statistics

This field displays the router's traffic statistics.

#### 5. System Up Time

The time of the router running from it's powered on or reset.

Router Status

LAN

MAC Address:

00-0A-EB-C9-98-76

IP Address:

192.168.1.1

Subnet Mask:

255.255.255.0

Wireless

Wireless Radio:

Enabled

SSID:

TP-LINK

Channel:

6

Mode:

54Mbps (802.11g)

MAC Address:

00-0A-EB-C9-98-76

IP Address:

192.168.1.1

WAN

MAC Address:

00-0A-EB-C9-98-77

IP Address:

0.0.0.0

PPPoE

Subnet Mask:

0.0.0.0

Default Gateway:

0.0.0.0

DNS Server:

Online Time:

0 day 00:00:00

Connect

Disconnect

Traffic Statistics

Received

Send

Bytes:

0

1368

Packets:

0

22

System Up Time:

1 day(s) 20:30:15

Refresh

Figure 5-1: Router Status

## 5.3 Quick Setup

Please refer to [Section 4.2: "Quick Installation Guide."](#)

## 5.4 Network



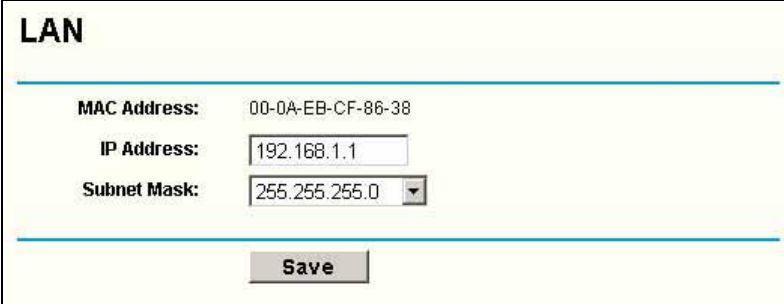
Figure 5-2: the Network menu

There are three submenus under the Network menu (shown in figure 5-2): **LAN**, **WAN** and **MAC Clone**. Click any of them, and you will be able to configure the corresponding function. The detailed explanations for each submenu are provided below.



### 5.4.1 LAN

You can configure the IP parameters of LAN on this page.



The screenshot shows a web interface for LAN configuration. At the top, the title "LAN" is displayed. Below it, there are three configuration fields: "MAC Address" with the value "00-0A-EB-CF-86-38", "IP Address" with the value "192.168.1.1", and "Subnet Mask" with the value "255.255.255.0". A "Save" button is located at the bottom of the form.

Figure 5-3: LAN

- **MAC Address** - the physical address of the router, as seen from the LAN. The value can't be changed.
- **IP Address** - Enter the IP address of your router in dotted-decimal notation (factory default: 192.168.1.1).
- **Subnet Mask** - An address code that determines the size of the network. Normally use 255.255.255.0 as the subnet mask.

**Note:**

- a. If you change the IP Address of LAN, you must use the new IP Address to login the router.
- b. If the new LAN IP Address you set is not in the same subnet, the IP Address pool in the DHCP sever will not take effect, until they are re-configured.
- c. If the new LAN IP Address you set is not in the same subnet, the Virtual Server and DMZ Host will change accordingly at the same time.

### 5.4.2 WAN

You can configure the WAN port parameters on this page.

First, please choose the WAN Connection Type (Dynamic IP/Static IP/PPPoE/802.1x + Dynamic IP/802.1x + Static IP) to the Internet. The default type is **PPPoE**. If you aren't given any login parameters (fixed IP Address, logging ID, etc), please select **Dynamic IP**. If you are given a fixed IP (static IP), please select **Static IP**. If you are given a user name and a password, please select PPPoE. If you are not sure which connection type you use currently, please contact your ISP to obtain the correct information.

1. If you choose **Dynamic IP**, the router will automatically get IP parameters from your ISP. You can see the page as follows (figure 5-4):

**WAN**

---

WAN Connection Type:

IP Address:

Subnet Mask:

Default Gateway:

MTU Size (in bytes):  (The default is 1500, do not change unless necessary.)

☐ Use These DNS Servers

Primary DNS:

Secondary DNS:  (Optional)

☐ Get IP with Unicast DHCP (It is usually not required.)

---

Figure 5-4 WAN – Dynamic IP

This page displays the WAN IP parameters assigned dynamically by your ISP, including IP address, Subnet Mask, Default Gateway, etc. Click the **Renew** button to renew the IP parameters from your ISP. Click the **Release** button to release the IP parameters.

**MTU Size:** The normal MTU (Maximum Transmission Unit) value for most Ethernet networks is 1500 Bytes. For some ISPs you need to reduce the MTU. But this is rarely required, and should not be done unless you are sure it is necessary for your ISP connection.

If your ISP gives you one or two DNS addresses, select **Use These DNS Servers** and enter the primary and secondary addresses into the correct fields. Otherwise, the DNS servers will be assigned dynamically from ISP.

**Note:** If you get 'Address not found' errors when you go to a Web site, it is likely that your DNS servers are set up improperly. You should contact your ISP to get DNS server addresses.

**Get IP with Unicast DHCP:** A few ISPs' DHCP servers do not support the broadcast applications. If you cannot get the IP Address normally, you can choose this option. (You generally need not check this option).

If you are also given a user name and a password for 802.1x authentication, you should select **802.1x + Dynamic IP** for **WAN Connection Type**, and a user name and a password will then appear, shown in figure 5-4a:

Figure 5-4a: WAN - 802.1X + Dynamic IP

- **User Name** - Enter the user name for 802.1x authentication provided by your ISP
  - **Password** - Enter the password for 802.1x authentication provided by your ISP.
- Click **Login** button to start 802.1x authentication.  
Click **Logout** button to end 802.1x authentication.
2. If you choose **Static IP**, you should have fixed IP Parameters specified by your ISP.  
The Static IP settings page will appear, shown in figure 5-5:

Figure 5-5: WAN - Static IP

You should type the following parameters into the spaces provided:

- **IP Address** - Enter the IP address in dotted-decimal notation provided by your ISP.
- **Subnet Mask** - Enter the subnet Mask in dotted-decimal notation provided by your ISP, usually is 255.255.255.0.
- **Default Gateway** - (Optional) Enter the gateway IP address in dotted-decimal notation provided by your ISP.
- **MTU Size** - The normal MTU (Maximum Transmission Unit) value for most Ethernet networks is 1500 Bytes. For some ISPs you may need to modify the MTU. But this is rarely required, and should not be done unless you are sure it is necessary for your ISP connection.
- **Primary DNS** - (Optional) Enter the DNS address in dotted-decimal notation provided by your ISP.
- **Secondary DNS** - (Optional) Type another DNS address in dotted-decimal notation provided by your ISP if provided.

If you are also given a user name and a password for 802.1x authentication, you should select **802.1x + Static IP** for **WAN Connection Type**, a box will then appear requesting a user name and a password, shown in figure 5-5a:

Figure 5-5a: WAN - 802.1X + Static IP

- **User Name** - Enter the user name for 802.1x authentication provided by your ISP
- **Password** - Enter the password for 802.1x authentication provided by your ISP.

Click **Login** to start 802.1x authentication.

Click **Logout** to end 802.1x authentication.

3. If you choose **PPPoE**, you should enter the following parameters (figure 5-6):

Figure 5-6: WAN - PPPoE

- **User Name/Password** - Enter the User Name and Password provided by your ISP. These fields are case-sensitive.
- **Connect on Demand** - You can configure the router to disconnect your Internet connection after a specified period of inactivity (**Max Idle Time**). If your Internet connection has been terminated due to inactivity, **Connect on Demand** enables the router to automatically re-establish your connection as soon as you attempt to access the Internet again. If you wish to activate **Connect on Demand**, click the radio button. If you want your Internet connection to remain active at all times, enter 0 in the **Max Idle Time** field. Otherwise, enter the number of minutes you want to have elapsed before your Internet connection terminates.

**Caution:** Sometimes the connection cannot be disconnected although you specify a time to Max Idle Time, since some applications is visiting the Internet continually in the background.

- **Connect Automatically** - Connect automatically after the router is disconnected. To use this option, click the radio button.
- **Time-based Connecting** - You can configure the router to make it connect or disconnect based on time. Enter the start time in HH:MM for connecting and end time in HH:MM for disconnecting in the **Period of Time** fields.

**Note:** Only when you have set the system time on **System Tools -> Time** page, will the **Time-based Connecting** function can take effect.

- **Connect Manually** - You can configure the router to make it connect or disconnect manually. After a specified period of inactivity (**Max Idle Time**), the router will disconnect your Internet connection, and not be able to re-establish your connection automatically as soon as you attempt to access the Internet again. To use this option, click the radio button. If you want your Internet connection to remain active at all times, enter "0" in the **Max Idle Time** field. Otherwise, enter the number in minutes that you wish to have the Internet connecting last unless a new link is requested.

**Caution:** Sometimes the connection cannot be disconnected although you specify a time to Max Idle Time, since some applications is visiting the Internet continually in the background.

Click the **Connect** button to connect immediately, Click the **Disconnect** button to disconnect immediately.

Click the **Advanced Settings** button to set up the advanced option, the page shown in figure 5-7 will then appear:

**PPPoE Advanced Settings**

MTU Size (in bytes):  (The default is 1492, do not change unless necessary.)

Service Name:

AC Name:

☐ Use IP address specified by ISP

ISP specified IP Address:

Detect Online Interval:  Seconds (0 ~ 120 seconds, 0 means do not detect.)

☐ Use These DNS Servers

Primary DNS:

Secondary DNS:  (Optional)

Figure 5-7: PPPoE Advanced Settings

- **Packet MTU** - The default MTU size is 1492 bytes, which value is usually fine. For some ISPs, you need modify the MTU. This should not be done unless you are sure

it is necessary for your ISP.

- **Service Name/AC Name** - The service name and AC (Access Concentrator) name, this should not be done unless you are sure it is necessary for your ISP.
- **ISP Specified IP Address** - If you know that your ISP does not automatically transmit your IP address to the router during login, click “**Use the IP Address specified by ISP**” check box and enter the IP Address in dotted-decimal notation, which your ISP provided.
- **Detect Online Interval** - The default value is 0, you can input the value between 0 and 120. The router will detect Access Concentrator online at every interval between seconds. If the value is 0, it means, do not detect.
- **DNS IP address** - If you know that your ISP does not automatically transmit DNS addresses to the router during login, click “**Use the following DNS servers**” checkbox and enter the IP address in dotted-decimal notation of your ISP’s primary DNS server. If a secondary DNS server address is available, enter it as well.

Click the **Save** button to save your settings.

### 5.4.3 MAC Clone

You can configure the MAC address of the WAN port on this page, figure 5-8:

MAC Clone	
WAN MAC Address:	<input type="text" value="00-0A-EB-CF-61-5D"/> <input type="button" value="Restore Factory MAC"/>
Your PC's MAC Address:	<input type="text" value="00-E0-4C-F3-8D-93"/> <input type="button" value="Clone MAC Address"/>
<input type="button" value="Save"/>	

Figure 5-8: MAC Address Clone

Some ISPs require that you register the MAC Address of your adapter, which is connected to your cable, DSL modem or Ethernet during installation. You do not generally need to change anything here.

- **WAN MAC Address** - This field displays the current MAC address of the WAN port, which is used for the WAN port. If your ISP requires that you register the MAC address, please enter the correct MAC address into this field. The format for the MAC Address is XX-XX-XX-XX-XX-XX (X is any hexadecimal digit).
- **Your PC's MAC Address** - This field displays the MAC address of the PC that is managing the router. If the MAC address is required, you can click the **Clone MAC Address** button and this MAC address will fill in the **WAN MAC Address** field.

Click **Restore Factory MAC** to restore the MAC address of WAN port to the factory default value.

Click the **Save** button to save your settings.

#### Note:

- 1) Only the PC(s) on your LAN can use the **MAC Address Clone** feature.
- 2) If you click the **Save** button, the router will prompt you to reboot.

## 5.5 Wireless



Figure 5-9: Wireless menu

There are three submenus under the Wireless menu (shown in figure 5-9): **Wireless Settings**, **MAC Filtering** and **Wireless Statistics**. Click any of them, and you will be able to configure the corresponding function. The detailed explanations for each submenu are provided below.

### 5.5.1 Wireless Settings

The basic settings for the wireless network are set on this page, figure 5-10:

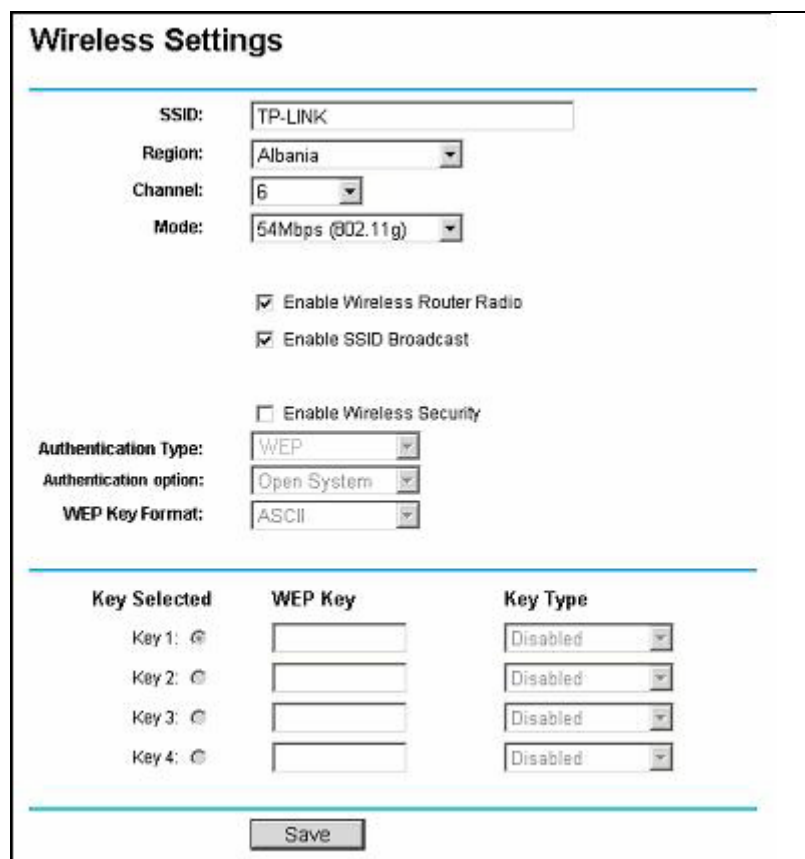
A screenshot of the 'Wireless Settings' configuration page. The page has a title 'Wireless Settings' at the top. Below the title, there are several configuration fields: 'SSID' (text box with 'TP-LINK'), 'Region' (dropdown menu with 'Albania'), 'Channel' (dropdown menu with '6'), and 'Mode' (dropdown menu with '54Mbps (802.11g)'). Below these are three checkboxes: 'Enable Wireless Router Radio' (checked), 'Enable SSID Broadcast' (checked), and 'Enable Wireless Security' (unchecked). Below the checkboxes are three more dropdown menus: 'Authentication Type' (set to 'WEP'), 'Authentication option' (set to 'Open System'), and 'WEP Key Format' (set to 'ASCII'). At the bottom, there is a table with three columns: 'Key Selected', 'WEP Key', and 'Key Type'. The table has four rows for 'Key 1', 'Key 2', 'Key 3', and 'Key 4'. Each row has a radio button in the 'Key Selected' column, an empty text box in the 'WEP Key' column, and a dropdown menu in the 'Key Type' column (all set to 'Disabled'). At the very bottom of the page is a 'Save' button.

Figure 5-10: Wireless Settings

- **SSID** - Enter a value of up to 32 characters. The same name (SSID) must be assigned to all wireless devices in your network. The default SSID is default, but it is recommended strongly that you change your networks name (SSID) to a different value. This value is case-sensitive. For example, *DEFAULT* is NOT the same as *default*.
- **Region** - Select your region from the pull-down list. This field specifies the region where the wireless function of the router can be used. It may be illegal to use the

wireless function of the router in a region other than one of those specified in this field. If your country or region is not listed, please contact your local government agency for assistance

**Note:** Some regions may not use **108Mbps Mode** since the operation for the wireless interface in 108Mbps Mode is illegal.

- **Channel** - This field determines which operating frequency will be used. It is not necessary to change the wireless channel unless you notice interference problems with another nearby access point.
- **Mode** - Select the desired wireless mode. The options are:
  - **108Mbps (Dynamic)** - Super G<sup>TM</sup>, 802.11g and 802.11b wireless stations can connect to the router.
  - **108Mbps (Static)** - Only Super G<sup>TM</sup> wireless stations can connect to the router.
  - **54Mbps (802.11g)** - Both 802.11g and 802.11b wireless stations can connect to the router.
  - **11Mbps (802.11b)** - Only 802.11b wireless stations can connect to the router.

**Note:** The default is "54Mbps (802.11g)", which allows both 802.11g and 802.11b wireless stations to connect to the router.

- **Enable Wireless Router Radio** - The wireless radio of this Router can be enabled or disabled to allow wireless stations access. If enabled, wireless stations will be able to access the router, otherwise, wireless stations will not be able to access the router.
- **Enable SSID Broadcast** - If you select the **Enable SSID Broadcast** checkbox, the Wireless Router SSID will broadcast its name (SSID) on the air.
- **Enable Wireless Security** – The wireless security function can be enabled or disabled. If disabled, the wireless stations will be able to connect the router without encryption. It is strongly recommended that you choose this optional to encrypt your wireless network. The encryption settings described below.
- **Authentication Type** - You can select one of the following authentication types:
  - **WEP** - Select WEP authentication type based on 802.11 authentication.
  - **WPA-PSK/WPA2-PSK** - Select WPA/WPA2 authentication type based on pre-shared passphrase.
  - **WPA /WPA2** - Select WPA/WPA2 authentication type based on Radius Server.
- **Authentication Option** - You can select one of the following authentication options:
  - When you select **WEP** as an authentication type you can select following authentication option:
  - **Automatic** - Select Shared Key or Open System authentication type automatically based on the wireless station request.
  - **Shared Key** - Select 802.11 Shared Key authentication.
  - **Open System** - Select 802.11 Open System authentication.
  - When you select **WPA-PSK/WPA2-PSK** for authentication type you can select



- **Automatic** , **WPA –PSK** or **WPA2-PSK** as authentication options.
  - When you select **WPA/WPA2** as an authentication type you can select **Automatic** , **WPA** or **WPA2** as authentication options.
- **WEP Key Format** - You can select **ASCII** or **Hexadecimal** format. ASCII Code Format stands for any combination of keyboard characters in a specified length. Hexadecimal format stands for any combination of hexadecimal digits (0-9, a-f, A-F) in a specified length.
- **WEP Key settings** - Select which of the four keys will be used and enter the matching WEP key information for your network in the selected key radio button. These values must be identical on all wireless stations in your network.
- **Key Type** - You can select the WEP key length (**64-bit**, or **128-bit**, or **152-bit**) for encryption. "Disabled" means the WEP key entry is invalid.
- For **64-bit** encryption - You can enter 10 hexadecimal digits (any combination of 0-9, a-f, A-F, zero key is not permitted) or 5 ASCII characters.
  - For **128-bit** encryption - You can enter 26 hexadecimal digits (any combination of 0-9, a-f, A-F, zero key is not permitted) or 13 ASCII characters.
  - For **152-bit** encryption - You can enter 32 hexadecimal digits (any combination of 0-9, a-f, A-F, zero key is not permitted) or 16 ASCII characters.
- **Encryption** - When you select **WPA-PSK/WPA2-PSK** or **WPA/WPA2** as **Authentication Types** you can select either **Automatic**, **TKIP** or **AES** as **Encryptions**.

Authentication Type:	WPA-PSK/WPA
Authentication option:	Automatic
Encryption:	Automatic
WPA-PSK Passphrase:	<input type="text"/>
	(The Passphrase is between 8 and 63 characters long)
Group Key Update Period:	30 (in seconds, minimum is 30 seconds, 0 means no update)

Figure 5-10a: WPA-PSK/WPA2-PSK

- **WPA-PSK/WPA2-PSK Passphrase** - You can enter a WPA or WPA2 passphrase between 8 and 63 characters long.
- **Group Key Update Period** - Specify the group key update interval in seconds. The value can be either 0 seconds or from 30 seconds and up, 1-29 seconds are not usable figures. Enter 0 to disable the update.

Authentication Type:	WPA/WPA2
Authentication option:	Automatic
Encryption:	Automatic
Radius Server IP:	<input type="text"/>
Radius Port:	1812 (1-65535, 0 means the default port 1812)
Radius password:	<input type="text"/>
Group Key Update Period:	30 (in seconds, minimum is 30 seconds, 0 means no update)

Figure 5-10b: WPA/WPA2

- **Radius Server IP** - Enter the IP address of the Radius Server

- **Radius Port** - Enter the port that the radius service used.
- **Radius Password** - Enter the password for the Radius Server.

Be sure to click the **Save** button to save your settings on this page.

**Note:** The router will reboot automatically after you click **save**.

### 5.5.2 MAC Filtering

The Wireless MAC Filtering for wireless networks are set on this page, figure 5-11:

Figure 5-11: Wireless MAC address Filtering

The Wireless MAC Address Filtering feature allows you to control wireless stations accessing the router, which depend on the station's MAC addresses.

- **MAC Address** - The wireless station's MAC address that you want to access.
- **Description** - A simple description of the wireless station.
- **Privilege** - **Allow** means allowing the station to access the router. **Deny** means denying the station to access the router. **64-bit**, or **128-bit**, or **152-bit** means assigning a unique WEP key to access the router.
- **WEP Key** - Specify a unique WEP key (in Hexadecimal format) to access the router.
- **Status** - The status of this entry, either **Enabled** or **Disabled**.

To disable the Wireless MAC Address Filters feature, keep the default setting, **Disable**.

To set up an entry, click **Enable**, and follow these instructions:

First, you must decide whether the unspecified wireless stations can or cannot access the router. If you desire that the unspecified wireless stations can access the router, please select the radio button **Allow the stations not specified by any enabled entries in the list to access**, otherwise, select the radio button **Deny the stations not specified by any enabled entries in the list to access**.

To Add a Wireless MAC Address filtering entry, click the **Add New...** button. The " **Add or Modify Wireless MAC Address Filtering entry**" page will appear, shown in figure 5-12:

**Add or Modify Wireless MAC Address Filtering entry**

MAC Address:

Description:

Privilege:

WEP Key:

Status:

Figure 5-12: Add or Modify Wireless MAC Address Filtering entry

To add or modify a MAC Address Filtering entry, follow these instructions:

1. Enter the appropriate MAC Address into the **MAC Address** field. The format of the MAC Address is XX-XX-XX-XX-XX-XX (X is any hexadecimal digit). For example: 00-0A-EB-B0-00-0B.
2. Enter a simple description of the wireless station in the **Description** field. For example: Wireless station A.
3. **Privilege** - Selects the privileges for this entry, one of **Allow** / **Deny** / **64-bit** / **128-bit** / **152-bit**.
4. **WEP Key** - If you select **64-bit**, **128-bit** or **152-bit** in the **Privilege** field, enter any combination of hexadecimal digits (0-9, a-f, A-F) in the specified length. For example: 2F34D20BE2.
5. **Status** - Select **Enabled** or **Disabled** for this entry on the **Status** pull-down list.
6. Click the **Save** button to save this entry.

To add additional entries, repeat steps 1-6.

**Note:** When 64-bit, or 128-bit, or 152-bit is selected, WEP Key will be enabled.

To modify or delete an existing entry:

1. Click the **Edit** or **Delete** button in the **Modify** column in the MAC Address Filtering Table.
2. Enter the value as desired in the **Add or Modify Wireless MAC Address Filtering entry** page, and click the **Save** button.

You can click the **Enable All** button to make all the entries effective, click the **Disable All** button to make all the entries ineffective, click the **Delete All** button to delete all the entries.

Click the **Next** button to go to the next page and click the **Previous** button to return to the previous page.

**For example:** If you desire that the wireless station A with MAC address 00-0A-EB-00-07-BE be able to access the router, the wireless station B with MAC address 00-0A-EB-00-07-5F not be able to access the router, and the wireless station C with MAC address 00-0A-EB-00-07-8A be able to access the router when its WEP key is 2F34D20BE2E54B326C5476586A, while all other wireless stations cannot access the router, you should configure the **Wireless MAC Address Filtering** list following these steps:

1. Click the **Enable** button to enable this function.
2. Select the radio button: **Deny the stations not specified by any enabled entries in the list to access** for **Filtering Rules**.
3. Delete all or disable all entries if there exist any entries already.
4. Click the **Add New...** button and enter the MAC address 00-0A-EB-00-07-BE in the **MAC Address** field, enter wireless station A in the **Description** field, select **Allow** in the **Privilege** pull-down list and select **Enabled** in the **Status** pull-down list. Click the **Save** and the **Return** button.
5. Click the **Add New...** button and enter the MAC address 00-0A-EB-00-07-5F in the **MAC Address** field, enter wireless station B in the **Description** field, select **Deny** in the **Privilege** pull-down list and select **Enabled** in the **Status** pull-down list. Click the **Save** and the **Return** button.
6. Click the **Add New...** button and enter the MAC address 00-0A-EB-00-07-8A in the **MAC Address** field, enter wireless station C in the **Description** field, select **128-bit** in the **Privilege** pull-down list, enter 2F34D20BE2E54B326C5476586A in the **WEP Key** field and select **Enabled** in the **Status** pull-down list. Click the **Save** and the **Return** button.

The filtering rules that configured should be similar to the following list:

ID	MAC Address	Status	Privilege	<input checked="" type="radio"/> Description <input type="radio"/> WEP Key	Modify
1	00-0A-EB-00-07-BE	Enabled	allow	Wireless Station A	<a href="#">Modify</a> <a href="#">Delete</a>
2	00-0A-EB-00-07-5F	Enabled	deny	Wireless Station B	<a href="#">Modify</a> <a href="#">Delete</a>
3	00-0A-EB-00-07-8A	Enabled	128 bit	Wireless Station C	<a href="#">Modify</a> <a href="#">Delete</a>

**Note:**

- a) If you select the radio button **Allow the stations not specified by any enabled entries in the list to access** for **Filtering Rules**, the wireless station B will still not be able to access the router, however, other wireless stations that are not in the list will be able to access the router.
- b) If you enable the function and select the **Deny the stations not specified by any enabled entries in the list to access** for **Filtering Rules**, and there are not any enable entries in the list, thus, no wireless stations can access the router.

### 5.5.3 Wireless Statistics

This page shows **MAC Address**, **Current Status**, **Received Packets** and **Sent Packets** for each connected wireless station.

Wireless Statistics				
Number of connected Wireless Stations:		0	<input type="button" value="Refresh"/>	
ID	MAC Address	Current Status	Received Packets	Sent Packets
<input type="button" value="Previous"/> <input type="button" value="Next"/>				

Figure 5-13: The router attached wireless stations

- **MAC Address** - The connected wireless station's MAC address
- **Current Status** - The connected wireless station's running status, one of STA-AUTH / STA-ASSOC / AP-UP / WPA / WPA-PSK / WPA2/WPA2-PSK/None
- **Received Packets** - packets received by the station
- **Sent Packets** - packets sent by the station

You cannot change any of the values on this page. To update this page and to show the current connected wireless stations, click on the **Refresh** button.

If the numbers of connected wireless stations go beyond one page, click the **Next** button to go to the next page and click the **Previous** button to return the previous page.

**Note:** This page will be refreshed automatically every 5 seconds.

## 5.6 DHCP

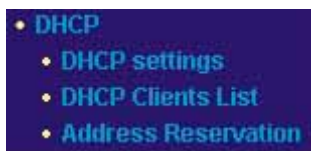


Figure 5-14: the DHCP menu

There are three submenus under the DHCP menu (shown in figure 5-14): **DHCP Settings**, **DHCP Clients List** and **Address Reservation**. Click any of them, and you will be able to configure the corresponding function. The detailed explanations for each submenu are provided below.

### 5.6.1 DHCP Settings

The router is set up by default as a DHCP (Dynamic Host Configuration Protocol) server, which provides the TCP/IP configuration for all the PCs that are connected to the router on the LAN. The DHCP Server can be configured on the page (shown in figure 5-15):

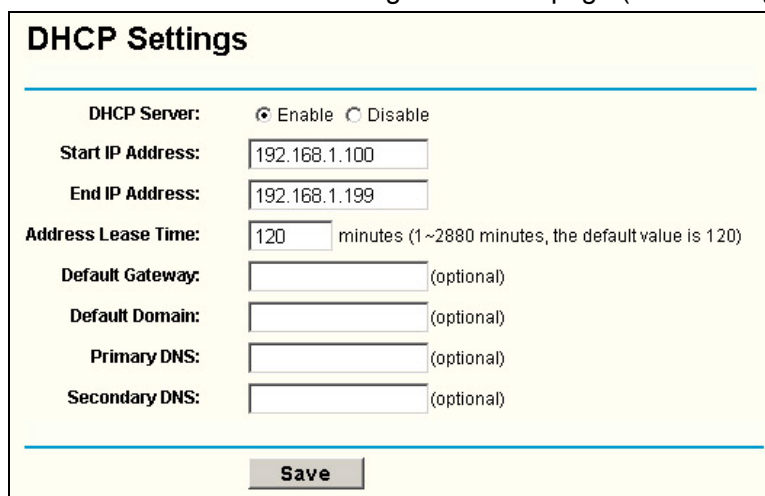
A screenshot of a web form titled 'DHCP Settings'. The form has a light yellow background and a blue border. It contains several configuration options: 'DHCP Server' with radio buttons for 'Enable' (selected) and 'Disable'; 'Start IP Address' with a text box containing '192.168.1.100'; 'End IP Address' with a text box containing '192.168.1.199'; 'Address Lease Time' with a text box containing '120' and a note 'minutes (1~2880 minutes, the default value is 120)'; 'Default Gateway' with a text box and '(optional)'; 'Default Domain' with a text box and '(optional)'; 'Primary DNS' with a text box and '(optional)'; and 'Secondary DNS' with a text box and '(optional)'. At the bottom of the form is a 'Save' button.

Figure 5-15: DHCP Settings

- **DHCP Server - Enable or Disable** the DHCP server. If you disable the Server, you must have another DHCP server within your network or else you must manually configure the computer.
- **Start IP Address** - This field specifies the first of the addresses in the IP address pool. 192.168.1.100 is the default start address.
- **End IP Address** - This field specifies the last of the addresses in the IP address pool. 192.168.1.199 is the default end address.
- **Address Lease Time** - The **Address Lease Time** is the amount of time a network user will be allowed connection to the router with their current dynamic IP Address. Enter the amount of time, in minutes, the user will be "leased" this dynamic IP Address. The range of the time is 1 ~ 2880 minutes. The default value is 120 minutes.
- **Default Gateway** - (Optional.) Suggest to input the IP address of the LAN port of the router, default value is 192.168.1.1
- **Default Domain** - (Optional.) Input the domain name of your network.
- **Primary DNS** - (Optional.) Input the DNS IP address provided by your ISP. Or consult your ISP.
- **Secondary DNS** - (Optional.) Input the IP address of another DNS server if your ISP provides two DNS servers.

**Note:** To use the DHCP server function of the router, you must configure all computers on the LAN as "Obtain an IP Address automatically" mode. This function will take effect until the router reboots.

### 5.6.2 DHCP Clients List

This page shows **Client Name**, **MAC Address**, **Assigned IP** and **Lease Time** for each DHCP Client attached to the router (figure 5-16):

DHCP Clients List				
Index	Client Name	MAC Address	Assigned IP	Lease Time
1	TP-7XXSIHL12MYS	00-0A-EB-00-00-08	192.168.1.100	01:59:52
<div>Refresh</div>				

Figure 5-16: DHCP Clients List

- **Index** - The index of the DHCP Client
- **Client Name** - The name of the DHCP client
- **MAC Address** - The MAC address of the DHCP client
- **Assigned IP** - The IP address that the router has allocated to the DHCP client.
- **Lease Time** - The time of the DHCP client leased. Before the time is up, DHCP client will request to renew the lease automatically.

You cannot change any of the values on this page. To update this page and to show the current attached devices, click on the **Refresh** button.

### 5.6.3 Address Reservation

When you specify a reserved IP address for a PC on the LAN, that PC will always receive the same IP address each time when it accesses the DHCP server. Reserved IP addresses should be assigned to servers that require permanent IP settings. This page is used for address reservation (shown in figure 5-17).

ID	MAC Address	Reserved IP Address
1	<input type="text"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>
5	<input type="text"/>	<input type="text"/>
6	<input type="text"/>	<input type="text"/>
7	<input type="text"/>	<input type="text"/>
8	<input type="text"/>	<input type="text"/>

Figure 5-17: Address Reservation

- **MAC Address** - The MAC address of the PC of which you want to reserve IP address.
- **Assigned IP Address** - The IP address of the router reserved.

#### To Reserve IP addresses:

1. Enter the MAC address (The format for the MAC Address is XX-XX-XX-XX-XX-XX.) and IP address in dotted-decimal notation of the computer you wish to add.
2. Click the **Save** button when finished.

#### To modify A Reserved IP address:

1. Select the reserved address entry as you desire, and modify it. If you wish to delete the entry, make all of the entry fields blank.
2. Click the **Save** button.

#### To delete all Reserved IP addresses:

1. Click the **Clear All** button.
2. Click the **Save** button

Click the **Next** button to go to the next page and Click the **Previous** button to return the previous page.

**Note:** The function won't take effect until the router reboots.

## 5.7 Forwarding

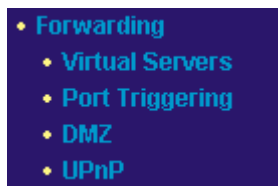


Figure 5-18: the Forwarding menu

There are four submenus under the Forwarding menu (shown in figure 5-18): **Virtual Servers**, **Port Triggering**, **DMZ** and **UPnP**. Click any of them, and you will be able to configure the corresponding function. The detailed explanations for each submenu are provided below.

### 5.7.1 Virtual Servers

Virtual servers can be used for setting up public services on your LAN, such as DNS, Email and FTP. A virtual server is defined as a service port, and all requests from Internet to this service port will be redirected to the computer specified by the server IP. Any PC that was used for a virtual server must have a static or reserved IP Address because its IP Address may change when using the DHCP function. You can set up virtual servers on this page, shown in figure 5-19:

A screenshot of the 'Virtual Servers' configuration page in a router's web interface. The page has a title 'Virtual Servers' at the top. Below it is a table with 5 columns: 'ID', 'Service Port', 'IP Address', 'Protocol', and 'Enable'. There are 8 rows in the table, each with input fields for the first four columns and a checkbox for the 'Enable' column. The 'IP Address' field in each row is pre-filled with '192.168.1.'. Below the table, there is a 'Common Service Port' section with a dropdown menu showing 'DNS(53)', a 'Copy to' button, and an 'ID' dropdown menu showing '1'. At the bottom of the page are four buttons: 'Previous', 'Next', 'Clear All', and 'Save'.

Figure 5-19: Virtual Servers

- **Service Port** - The numbers of External Ports. You can type a service port or a range of service ports (the format is XXX – YYY, XXX is Start port, YYY is End port).
- **IP Address** - The IP Address of the PC running the service application
- **Protocol** - The protocol used for this application, either **TCP**, **UDP**, or **All** (all



protocols supported by the router).

- **Enable** - The Enable checkbox to enable the virtual server entry.
- **Common Service Port** - Some common services already list in the pull-down list.

#### **To setup a virtual server entry:**

1. Select the service you want to use from the Common Service Port list, and select the ID you want to use, and click **Copy to** button. If the **Common Service Port** list does not have the service that you want to use, type the number of the service port or service port range in the **Service Port** box.
2. Type the IP Address of the computer in the **Server IP Address** box.
3. Select the protocol used for this application, either **TCP** or **UDP**, or **All**.
4. Select the **Enable** checkbox to enable the virtual server.
5. Click the **Save** button.

**Note:** It is possible that you have a computer or server that has more than one type of available service. If so, select another service, and enter the same IP Address for that computer or server.

#### **To modify a virtual server entry:**

1. Select the entry you want to modify.
2. Modify the information from the **Service Port**, the **IP Address** boxes, and the **Protocol** pull-down list.
3. Click the **Save** button.

#### **To delete a service entry:**

1. Clear the entry's all information except the **Protocol** pull-down list.
2. Click the **Save** button.

#### **To delete all service entries:**

1. Click the **Clear All** button.
2. Click the **Save** button

Click the **Next** button to go to the next page and Click the **Previous** button to return the previous page.

**Note:** If you set the virtual server of service port as 80, you must set the web management port on **Security → Remote Management** page to be any value except 80 such as 8080. Or else there will be a conflict to disable the virtual server.

### **5.7.2 Port Triggering**

Some applications require multiple connections, like Internet games, video conferencing, Internet calling and so on. These applications cannot work with a pure NAT router. Port Triggering is used for some of these applications that can work with an NAT router. You can set up Port Triggering on this page shown in figure 5-20:

Port Triggering					
ID	Trigger Port	Trigger Protocol	Incoming Ports Range	Incoming Protocol	Enable
1	<input type="text"/>	ALL	<input type="text"/>	ALL	<input type="checkbox"/>
2	<input type="text"/>	ALL	<input type="text"/>	ALL	<input type="checkbox"/>
3	<input type="text"/>	ALL	<input type="text"/>	ALL	<input type="checkbox"/>
4	<input type="text"/>	ALL	<input type="text"/>	ALL	<input type="checkbox"/>
5	<input type="text"/>	ALL	<input type="text"/>	ALL	<input type="checkbox"/>
6	<input type="text"/>	ALL	<input type="text"/>	ALL	<input type="checkbox"/>
7	<input type="text"/>	ALL	<input type="text"/>	ALL	<input type="checkbox"/>
8	<input type="text"/>	ALL	<input type="text"/>	ALL	<input type="checkbox"/>

Common Applications:   ID

Figure 5-20: Port Triggering

Once configured, operation is as follows:

1. A local host makes an outgoing connection using a destination port number defined in the Trigger Port field.
2. The router records this connection, opens the incoming port or ports associated with this entry in the Port Triggering table, and associates them with the local host.
3. When necessary the external host will be able to connect to the local host using one of the ports defined in the **Incoming Ports** field.

- **Trigger Port** - The port for outgoing traffic. An outgoing connection using this port will "Trigger" this rule.
- **Trigger Protocol** - The protocol used for Trigger Ports, either **TCP**, **UDP**, or **All** (all protocols supported by the router).
- **Incoming Ports Range** - The port or port range used by the remote system when it responds to the outgoing request. A response using one of these ports will be forwarded to the PC that triggered this rule. You can input at most 5 groups of ports (or port section). Every group of ports must be apart with ",". For example, 2000-2038, 2050-2051, 2085, 3010-3030.
- **Incoming Protocol** - The protocol used for Incoming Ports Range, either TCP or UDP, or ALL (all protocols supported by the router).
- **Enable** - The Enable checkbox enables port forwarding for the application.
- **Common Applications** - Some popular applications already list in the pull-down list.

To add a new rule, enter the following data on the **Port Triggering** screen.

1. Enter a port number used by the application when it generates an outgoing request.
2. Select the protocol used for **Trigger Port** from the pull-down list, either **TCP**, **UDP**, or **All**.
3. Enter the range of port numbers used by the remote system when it responds to the PC's request.

4. Select the protocol used for **Incoming Ports Range** from the pull-down list, either **TCP** or **UDP**, or **All**.
5. Select the **Enable** checkbox to enable.
6. Click the **Save** button to save the new rule.

There are many popular applications in the **Popular Application** list. You can select it and the ID, then click the **Copy to** button, the application will fill in the **Trigger Port**, **incoming Ports Range** boxes and select the **Enable** checkbox. It has the same effect as adding a new rule.

#### Modifying an existing rule:

1. Edit the entry as desired.
2. Click the **Save** button.

#### Deleting an existing rule:

1. Clear all the content in the **Trigger Port** field, the **Open Port** field and the **Enable** checkbox.
2. Click the **Save** button.

#### To delete all rules:

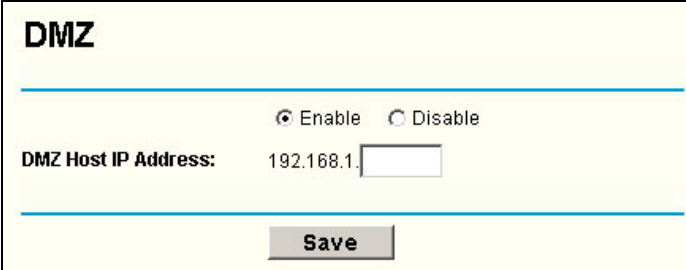
1. Click the **Clear All** button.
2. Click the **Save** button

#### Note:

1. When the trigger connection is released, the according opening ports will be closed.
2. Each rule allowed to be used only by one host on LAN synchronously. The trigger connection of other hosts on LAN will be refused.
3. Incoming Port Range cannot overlap each other.

### 5.7.3 DMZ

The DMZ host feature allows one local host to be exposed to the Internet for a special-purpose service such as Internet gaming or videoconferencing. DMZ host forwards all the ports at the same time. Any PC whose port is being forwarded must have its DHCP client function disabled and should have a new static IP Address assigned to it because its IP Address may change when using the DHCP function. You can set up DMZ host on this page shown in figure 5-21:



**DMZ**

☒ Enable ☐ Disable

DMZ Host IP Address: 192.168.1.

**Save**

Figure 5-21: DMZ

To assign a computer or server to be a DMZ server:

1. Click the **Enable** radio button
2. Enter the local host IP Address in the **DMZ Host IP Address** field
3. Click the **Save** button.

**Note:** After you set the DMZ host, the firewall related to the host will not work.

#### 5.7.4 UPnP

The Universal Plug and Play (UPnP) feature allows the devices, such as Internet computers, to access the local host resources or devices as needed. UPnP devices can be automatically discovered by the UPnP service application on the LAN. You can configure UPnP on this page that shown in figure 5-22:

UPnP						
Current UPnP Status: <b>Disabled</b> <input type="button" value="Enable"/>						
Current UPnP Settings List						
ID	App Description	External Port	Protocol	Internal Port	IP Address	Status
<input type="button" value="Refresh"/>						

Figure 5-22: UPnP Settings

- **Enable UPnP** - UPnP can be enabled or disabled by clicking the **Enable** or **Disable** button. As allowing this may present a risk to security, this feature is disabled by default.
- **Current UPnP Settings Table** - this table displays the current UPnP information.
  - **App Description** – The description provided by the application in the UPnP request
  - **External Port** - External port, which the router opened for the application.
  - **Protocol** - Which type of protocol is opened.
  - **Internal Port** - Internal port, which the router opened for local host.
  - **IP Address** - The UPnP device that is currently accessing the router.
  - **Status** - Either Enabled or Disabled, “Enabled” means that port is still active, otherwise, the port is inactive.

Click **Refresh** to update the Current UPnP Settings List.

## 5.8 Security



Figure 5-23: the Security menu

There are six submenus under the Security menu (shown in figure 5-23): **Firewall**, **IP Address Filtering**, **Domain Filtering**, **MAC Filtering**, **Remote Management** and **Advanced Security**. Click any of them, and you will be able to configure the corresponding function. The detailed explanations for each submenu are provided below.

### 5.8.1 Firewall

Using the Firewall page (shown in figure 5-24), you can turn the general firewall switch on or off. The default setting for the switch is off. If the general firewall switch is off, even if IP Address Filtering, DNS Filtering and MAC Filtering are enabled, their settings are ineffective.

A screenshot of the 'Firewall' configuration page. The title 'Firewall' is at the top left. Below it is a horizontal line. The page contains several settings: a checkbox for 'Enable firewall (the general firewall switch)', a checkbox for 'Enable IP Address Filtering', a section for 'Default IP Address Filtering Rules' with two radio button options ('Allow' and 'Deny'), a checkbox for 'Enable Domain Filtering', a checkbox for 'Enable MAC Address Filtering', a section for 'Default MAC Address Filtering Rules' with two radio button options ('Allow' and 'Deny'), and a 'Save' button at the bottom center.

Figure 5-24: Firewall Settings

- **Enable Firewall** - the general firewall switch is on or off.
- **Enable IP Address Filtering** - set IP Address Filtering is enabled or disabled. There are two default filtering rules of IP Address Filtering, either Allow or Deny passing through the router.
- **Enable Domain Filtering** - set Domain Filtering is enabled or disabled.

- **Enable MAC Filtering** - set MAC Address Filtering is enabled or disabled. You can select the default filtering rules of MAC Address Filtering, either Allow or Deny accessing the router.

### 5.8.2 IP Address Filtering

The IP address Filtering feature allows you to control Internet Access by specific users on your LAN based on their IP addresses. The IP address filtering are set on this page, figure 5-25:

ID	Effective time	LAN IP	LAN Port	WAN IP	WAN Port	Protocol	Pass	Status	Modify
1	0000-2400	192.168.1.7	-	-	25	ALL	No	Enabled	<a href="#">Modify</a> <a href="#">Delete</a>
2	0000-2400	192.168.1.7	-	-	110	ALL	No	Enabled	<a href="#">Modify</a> <a href="#">Delete</a>
3	0000-2400	192.168.1.8	-	202.96.134.12	-	ALL	No	Enabled	<a href="#">Modify</a> <a href="#">Delete</a>

Figure 5-25: IP address Filtering

To disable the IP Address Filtering feature, keep the default setting, **Disabled**. To set up an IP Address Filtering entry, click **Enable** Firewall and **Enable** IP Address Filtering on the Firewall page, and click the **Add New...** button. The page " **Add or Modify an IP Address Filtering entry** " will appear shown in figure 5-26:

Figure 5-26: Add or Modify an IP Address Filtering Entry

To create or modify an IP Address Filtering entry, please follow these instructions:

1. **Effective Time** - Enter a range of time in HHMM format, which point to the range time for the entry to take effect. For example, 0803 - 1705, the entry will take effect from 08:03 to 17:05.
2. **LAN IP Address** - type a LAN IP Address or a range of LAN IP addresses in the field, in dotted-decimal notation format. For example, 192.168.1.20 - 192.168.1.30.

- Keep the field open, which means all LAN IP Addresses have been put into the field.
3. **LAN Port** - type a LAN Port or a range of LAN ports in the field. For example, 1030 - 2000. Keep the field open, which means all LAN ports have been put into the field.
  4. **WAN IP Address** - type a WAN IP Address or a range of WAN IP Addresses in the field, in dotted-decimal notation format. For example, 61.145.238.6 – 61.145.238.47. Keep the field open, which means all WAN IP Addresses have been put into the field.
  5. **WAN Port** - type a WAN Port or a range of WAN Ports in the field. For example, 25 – 110. Keep the field open, which means all WAN Ports have been put into the field.
  6. **Protocol** - select which protocol is to be used, either **TCP**, **UDP**, or **All** (all protocols supported by the router).
  7. **Pass** - select either **Allow** or **Deny** through the router.
  8. **Status** - select **Enabled** or **Disabled** for this entry on the **Status** pull-down list.
  9. Click the **Save** button to save this entry.

To add additional entries, repeat steps 1-9.

When finished, click the **Return** button to return to **IP Address Filtering** page.

To modify or delete an existing entry:

1. Find the desired entry in the table.
2. Click **Modify** or **Delete** as desired on the **Modify** column.

Click the **Enable All** button to make all entries enabled

Click the **Disabled All** button to make all entries disabled.

Click the **Delete All** button to delete all entries

You can change the entry's order as desired. Fore entries are before hind entries. Enter the ID number in the first box you want to move and another ID number in second box you want to move to, and then click the **Move** button to change the entry's order.

Click the **Next** button to the next page and click the **Previous** button to return to the previous page.

**For example:** If you desire to block E-mail received and sent by the IP Address 192.168.1.7 on your local network, and to make the PC with IP Address 192.168.1.8 unable to visit the website of IP Address 202.96.134.12, while other PCs have no limit. You should specify the following IP address filtering list:

ID	Effective time	LAN IP	LAN Port	WAN IP	WAN Port	Protocol	Pass	Status	Modify
1	0000-2400	192.168.1.7	-	-	25	ALL	No	Enabled	<a href="#">Modify</a> <a href="#">Delete</a>
2	0000-2400	192.168.1.7	-	-	110	ALL	No	Enabled	<a href="#">Modify</a> <a href="#">Delete</a>
3	0000-2400	192.168.1.8	-	202.96.134.12	-	ALL	No	Enabled	<a href="#">Modify</a> <a href="#">Delete</a>

### 5.8.3 Domain Filtering

The Domain Filtering page (shown in figure 5-27) allows you to control access to certain websites on the Internet by specifying their domains or key words.

**Domain Filtering**

---

**Firewall Settings (You can change it on Firewall page)**

Enable Firewall: **Enabled**

Enable Domain Filtering: **Enabled**

ID	Effective time	Domain Name	Status	Modify
<input type="button" value="Add New..."/> <input type="button" value="Enable All"/> <input type="button" value="Disable All"/> <input type="button" value="Delete All"/>				

---

Figure 5-27: Domain Filtering

Before adding a Domain Filtering entry, you must ensure that **Enable** Firewall and **Enable** Domain Filtering have been selected on the Firewall page. To Add a Domain filtering entry, click the **Add New...** button. The page " **Add or Modify a Domain Filtering entry** " will appear, shown in figure 5-28:

**Add or Modify a Domain Filtering entry**

---

Effective time:  -

Domain Name:

Status:  ▼

---

Figure 5-28: Add or Modify a Domain Filtering entry

To add or modify a Domain Filtering entry, follow these instructions:

1. **Effective Time** - Enter a range of time in HHMM format, which point to the range time for the entry to take effect. For example, 0803 - 1705, the entry will take effect from 08:03 to 17:05.
2. **Domain Name** - Type the domain or key word as desired in the field. A blank in the domain field means all websites on the Internet. For example: [www.xxyy.com.cn](http://www.xxyy.com.cn), .net.
3. **Status** - Select **Enabled** or **Disabled** for this entry on the **Status** pull-down list.
4. Click the **Save** button to save this entry.

To add additional entries, repeat steps 1-4.

When finished, click the **Return** button to return to the **Domain filtering** page.

To Modify or delete an existing entry:

1. Find the desired entry in the table.
2. Click **Modify** or **Delete** as desired on the **Edit** column.

Click the **Enabled All** button to make all entries enabled.

Click the **Disabled All** button to make all entries disabled.

Click the **Delete All** button to delete all entries



Click the **Next** button to go to the next page and the **Previous** button to return to the previous page.

For example, if you want to block the PCs on your LAN to access websites [www.xxyy.com.cn](http://www.xxyy.com.cn), [www.aabbcc.com](http://www.aabbcc.com) and websites with .net in the end on the Internet while no limit for other websites, you should specify the following Domain filtering list:

ID	Effective time	Domain Name	Status	Modify
1	0000-2400	www.xxyy.com.cn	Enabled	<a href="#">Modify</a> <a href="#">Delete</a>
2	0800-2000	www.aabbcc.com	Enabled	<a href="#">Modify</a> <a href="#">Delete</a>
3	0000-2400	.net	Enabled	<a href="#">Modify</a> <a href="#">Delete</a>

#### 5.8.4 MAC Filtering

Like the IP Address Filtering page, the MAC Address Filtering page (shown in figure 5-29) allows you to control access to the Internet by users on your local network based on their MAC Address.

**MAC Address Filtering**

Firewall Settings (You can change it on Firewall page)

Enable Firewall: **Enabled**

Enable MAC Address Filtering: **Enabled**

Default Filtering Rules: **Allow these PCs with enabled rules to access the Internet**

ID	MAC Address	Description	Status	Modify
1	00-E0-4C-00-07-BE	John's computer	Enabled	<a href="#">Modify</a> <a href="#">Delete</a>
2	00-E0-4C-00-07-5F	Alice's computer	Disabled	<a href="#">Modify</a> <a href="#">Delete</a>
3	00-E0-4C-00-07-09	Mr Liu's computer	Enabled	<a href="#">Modify</a> <a href="#">Delete</a>

Add New... Enable All Disable All Delete All

Previous Next

Figure 5-29: MAC address Filtering

Before setting up MAC Filtering entries, you must ensure that **Enable** Firewall and **Enable** MAC Filtering have been selected on the Firewall page. To Add a MAC Address filtering entry, clicking the **Add New...** button. The page " **Add or Modify a MAC Address Filtering entry**" will appear, shown in figure 5-30:

**Add or Modify a MAC Address Filtering Entry**

MAC Address:

Description:

Status:

Save Return

Figure 5-30: Add or Modify a MAC Address Filtering entry

To add or modify a MAC Address Filtering entry, follow these instructions:

1. Enter the appropriate MAC Address into the **MAC Address** field. The format of the MAC Address is XX-XX-XX-XX-XX-XX (X is any hexadecimal digit). For example: 00-0E-AE-B0-00-0B.
2. Type the description of the PC in the **Description** field. Fox example: John's PC.
3. **Status** - Select **Enabled** or **Disabled** for this entry on the **Status** pull-down list.
4. Click the **Save** button to save this entry.

To add additional entries, repeat steps 1-4.

When finished, click the **Return** button to return to the **MAC Address Filtering** page.

To Modify or delete an existing entry:

1. Find the desired entry in the table.
2. Click **Modify** or **Delete** as desired on the **Edit** column.

Click the **Enable All** button to make all entries enabled.

Click the **Disabled All** button to make all entries disabled.

Click the **Delete All** button to delete all entries

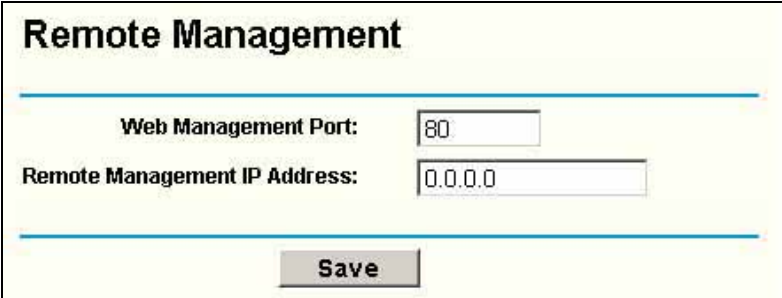
Click the **Next** button to go to the next page and click the **Previous** button to return to the previous page.

**Fox example:** If you want to block the PCs with MAC addresses 00-0A-EB-00-07-BE and 00-0A-EB-00-07-5F to access the Internet, first, enable the **Firewall** and **MAC Address Filtering** on the **Firewall** page, then, you should specify the Default MAC Address Filtering Rule "**Deny these PCs with effective rules to access the Internet**" on the Firewall page and the following MAC address filtering list on this page:

ID	MAC Address	Description	Status	Modify
1	00-0A-EB-00-07-BE	John's computer	Enabled	<a href="#">Modify</a> <a href="#">Delete</a>
2	00-0A-EB-00-07-5F	Alice's Computer	Enabled	<a href="#">Modify</a> <a href="#">Delete</a>

### 5.8.5 Remote Management

You can configure the Remote Management function on this page shown in figure 5-31. This feature allows you to manage your Router from a remote location, via the Internet.



**Remote Management**

Web Management Port:

Remote Management IP Address:

**Save**

Figure 5-31: Remote Management

- **Web Management Port** - Web browser access normally uses the standard HTTP service port 80. This router's default remote management web port number is 80. For greater security, you can change the remote management web interface to a custom port by entering that number in this box provided. Choose a number between 1024 and 65534, but do not use the number of any common service port.
- **Remote Management IP Address** - This is the current address you will use when accessing your router from the Internet. The default IP Address is 0.0.0.0. It means this function is disabled. To enable this function, change the default IP Address to another IP Address as desired.

To access the router, you will type your router's WAN IP Address into your browser's Address (in IE) or Location (in Navigator) box, followed by a colon and the custom port number. For example, if your Router's WAN address is 202.96.12.8 and you use port number 8080, enter in your browser: <http://202.96.12.8:8080>. You will be asked for the router's password. After successfully entering the password, you will be able to access the router's web-based utility.

**Note:** Be sure to change the router's default password to a very secure password.

### 5.8.6 Advanced Security

Using Advanced Security page (shown in figure 5-32), you can protect the router from being attacked by TCP-SYN Flood, UDP Flood and ICMP-Flood from LAN.

### Advanced Security

---

Packets Statistic interval (5 ~ 60):
Seconds

DoS protection:
☐ Disable
☒ Enable

☒ Enable ICMP-FLOOD Attack Filtering

ICMP-FLOOD Packets threshold (5 ~ 3600):
Packets/s

☒ Enable UDP-FLOOD Filtering

UDP-FLOOD Packets threshold (5 ~ 3600):
Packets/s

☒ Enable TCP-SYN-FLOOD Attack Filtering

TCP-SYN-FLOOD Packets threshold (5 ~ 3600):
Packets/s

☒ Ignore Ping Packet From WAN Port

☒ Forbid Ping Packet From LAN Port

Figure 5-32: Advanced Security settings

- **Packets Statistic interval (5 ~ 60)** - The default value is 10. Select a value between 5 and 60 seconds in the pull-down list. The **Packets Statistic interval** value indicates the time section of the packets statistic. The result of the statistic used for analysis by **SYN Flood**, **UDP Flood** and **ICMP-Flood**.
- **DoS protection - Enable or Disable** the DoS protection function. Only when it is enabled, will the flood filters be effective.
- **Enable ICMP-FLOOD Attack Filtering - Enable or Disable** the **ICMP-FLOOD** Attack Filtering.
- **ICMP-FLOOD Packets threshold: (5 ~ 3600)** - The default value is 50. Enter a value between 5 ~ 3600 packets. When the current **ICMP-FLOOD** Packets numbers is beyond the set value, the router will start up the blocking function immediately.
- **Enable UDP-FLOOD Filtering - Enable or Disable** the **UDP-FLOOD** Filtering.
- **UDP-FLOOD Packets threshold: (5 ~ 3600)** - The default value is 50. Enter a value between 5 ~ 3600 packets. When the current **UPD-FLOOD** Packets numbers is beyond the set value, the router will start up the blocking function immediately.
- **Enable TCP-SYN-FLOOD Attack Filtering - Enable or Disable** the **TCP-SYN-FLOOD** Attack Filtering.
- **TCP-SYN-FLOOD Packets threshold: (5 ~ 3600)** - The default value is 50. Enter a value between 5 ~ 3600 packets. When the current **TCP-SYN-FLOOD** Packets numbers is beyond the set value, the router will start up the blocking function immediately.
- **Ignore Ping Packet from WAN Port - Enable or Disable** ignore ping packet from WAN port. The default is disabled. If enabled, the ping packet from the Internet cannot access the router.
- **Forbid Ping Packet from LAN Port - Enable or Disable** forbidding Ping Packet to access the router from the LAN port. The default value is disabled. If enabled, the ping packet from the LAN port cannot access the router. (Defends against some viruses)

Click the **Save** button to save the settings.

Click the **Blocked DoS Host Table** button to display the DoS host table by blocking. The page will appear that shown in figure 5-33:

Blocked Host List		
ID	Host IP Address	Host MAC Address
<div> <input type="button" value="Refresh"/> <input type="button" value="Clear All"/> <input type="button" value="Return"/> </div>		

Figure 5-33: Thwarted DoS Host Table

This page shows **Host IP Address** and **Host MAC Address** for each host blocked by the router.

- **Host IP Address-** The IP address that blocked by DoS are displayed here.
- **Host MAC Address -** The MAC address that blocked by DoS are displayed here.

To update this page and to show the current blocked host, click on the **Refresh** button. Click the **Clear All** button to clear all displayed entries. After the table is empty the blocked host will regain the capability to access Internet.

Click the **Return** button to return to the **Advanced Security** page

## 5.9 Static Routing

A static route is a pre-determined path that network information must travel to reach a specific host or network. To add or delete a route, work in the area under the Static Routing page (shown in figure 5-34).

ID	Destination IP Address	Subnet Mask	Gateway	Enable
1	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
2	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
3	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
4	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
5	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
6	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
7	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
8	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>

Figure 5-34: Static Routing

### To add static routing entries:

- Enter the following data:
  - **Destination IP Address** - The **Destination IP Address** is the address of the network or host that you want to assign to a static route.
  - **Subnet Mask** - The **Subnet Mask** determines which portion of an IP Address is the network portion, and which portion is the host portion.
  - **Gateway** - This is the IP Address of the gateway device that allows for contact between the router and the network or host.
- Click the **Enable** checkbox.
- Repeat steps 1-2 until you are finished.
- If you are finished. Click the **Save** button to save it.

### To modify an existing entry:

- Modify the entry's **Destination IP Address**, **Subnet Mask** and **Gateway**.
- Click the **Save** button.

### To delete an existing entry:

- Select the entry as you desire and make all of its fields blank.
- Click the **Save** button.

**To delete all the entries:**

1. Click the **Clear All** button.
2. Click the **Save** button.

**Note:** You can set up to 8 entries.

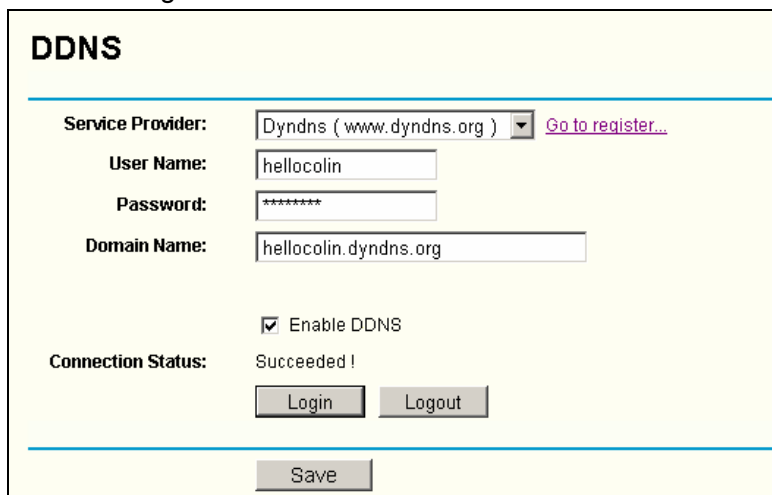
## 5.10 DDNS

The router offers a Dynamic Domain Name System (**DDNS**) feature. DDNS lets you assign a fixed host and domain name to a dynamic Internet IP Address. It is useful when you are hosting your own website, FTP server, or other server behind the router. Before using this feature, you need to sign up for DDNS service providers such as [www.dyndns.org](http://www.dyndns.org), [www.oray.net](http://www.oray.net) or [www.comexe.cn](http://www.comexe.cn). The Dynamic DNS client service provider will give you a password or key.

To set up for DDNS, follow these instructions:

### 5.10.1 Dyndns.org DDNS

If your selected dynamic DNS **Service Provider** is [www.dyndns.org](http://www.dyndns.org). The page will appear as shown in figure 5-35:



**DDNS**

**Service Provider:** Dyndns ( www.dyndns.org ) [Go to register...](#)

**User Name:** hellocolin

**Password:** \*\*\*\*\*

**Domain Name:** hellocolin.dyndns.org

☒ Enable DDNS

**Connection Status:** Succeeded!

Login Logout

Save

Figure 5-35: Dyndns.org DDNS Settings

To set up for DDNS, follow these instructions:

1. Type the **domain names** your dynamic DNS service provider gave.
  2. Type the **User Name** for your DDNS account.
  3. Type the **Password** for your DDNS account.
  4. Click the **Login** button to login to the DDNS service.
- **Connection Status** -The status of the DDNS service connection is displayed here. Click **Logout** to logout of the DDNS service.

### 5.10.2 Oray.net DDNS

If your selected dynamic DNS **Service Provider** is [www.oray.net](http://www.oray.net). The page will appear as shown in figure 5-36:

## DDNS

---

Service Provider:

www.oray.net

User Name:

hellocolin

Password:

\*\*\*\*\*

Connection Status:

Connected successfully.

Domain Name 1:

hellopig.vicp.net

2:

hellodog.vicp.net

3:

hellocat.vicp.net

4:

hellobinge.vicp.net

5:

hellocolin.vicp.net

Login

Logout

---

Save

Figure 5-36: Oray.net DDNS Settings

To set up for DDNS, follow these instructions:

1. Type the **User Name** for your DDNS account.
  2. Type the **Password** for your DDNS account.
  3. Click the **Login** button to login the DDNS service.
- **Connection Status** - the status of the DDNS service connection is displayed here.
  - **Domain Name** - the domain names are displayed here.

Click **Logout** to logout the DDNS service.

### 5.10.3 Comexe.cn DDNS

If your selected dynamic DNS **Service Provider** is [www.comexe.cn](http://www.comexe.cn). The page will appear as shown in figure 5-37:

**DDNS**

**Service Provider:**

**Domain Name 1:**

**Domain Name 2:**

**Domain Name 3:**

**Domain Name 4:**

**Domain Name 5:**

**User Name:**

**Password:**

**Connection Status:** Connecting...

Figure 5-37: Comexe.cn DDNS Settings

To set up for DDNS, follow these instructions:

5. Type the **domain names** your dynamic DNS service provider gave.
  6. Type the **User Name** for your DDNS account.
  7. Type the **Password** for your DDNS account.
  8. Click the **Login** button to login to the DDNS service.
- **Connection Status** -The status of the DDNS service connection is displayed here.

Click **Logout** to logout of the DDNS service.

## 5.11 System Tools



Figure 5-38: the System Tools menu

There are seven submenus under the System Tools menu (shown in figure 5-38): **Time**, **Firmware**, **Factory Defaults**, **Reboot**, **Password**, **Log** and **Statistics**. Click any of them, and you will be able to configure the corresponding function. The detailed explanations for each submenu are provided below.



### 5.11.1 Time

You can set time manually or get GMT from the Internet for the router on this page (shown in figure 5-39):

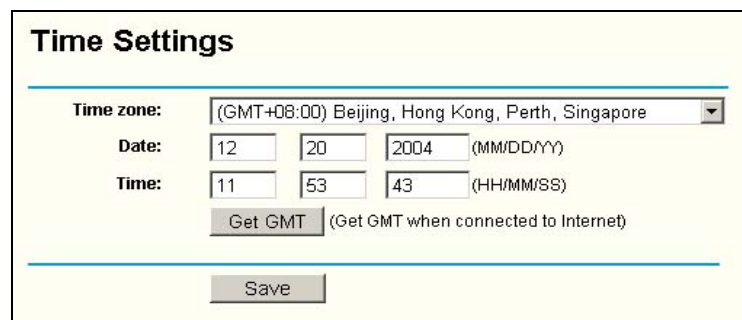


Figure 5-39: Time settings

- **Time Zone** - Select your local time zone from this pull down list.
- **Date** - Enter your local date in MM/DD/YY into the right blanks.
- **Time** - Enter your local time in HH/MM/SS into the right blanks.

Time setting follows these steps below:

1. Select your local time zone.
2. Enter date and time in the right blanks
3. Click **Save**.

Click the **Get GMT** button to get GMT time from Internet if you have connected to Internet.

#### Note:

1. This setting will be used for some time-based functions such as firewall. You must specify your time zone once you login to the router successfully, if not the time limited on these functions will not take effect.
2. The time will be lost if the router is turned off.
3. The router will obtain GMT automatically from Internet if it has already connected to Internet.

### 5.11.2 Firmware

The page (shown in figure 5-40) allows you to upgrade the latest version of firmware for the router.

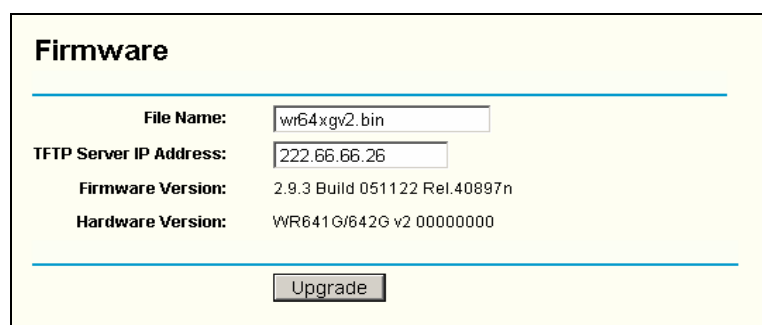


Figure 5-40: Firmware Upgrade

If the router is not experiencing difficulties, there is no need to download a more recent firmware version, unless that version has a new feature that you want to use.

**Note: When you upgrade the router's firmware, you may lose its configuration settings, so make sure you write down the router settings before you upgrade its firmware.**

To upgrade the router's firmware, follow these instructions:

1. Download a more recent firmware upgrade file.
  2. Run a TFTP Server on a PC on your LAN, and take the file in the TFTP server's path.
  3. Type the downloaded file name into the **File Name** box.
  4. Type the IP Address of the PC that runs the TFTP server in the **TFTP Server's IP Address** field.
  5. Click the **Upgrade** button.
- **Firmware Version** - displays the current firmware version.
  - **Hardware Version** - displays the current hardware version. The hardware version of the upgrade file must accord with the current hardware version.

**Note:**

1. **Do not turn off the router or press the Reset button while the firmware is being upgraded.**
2. The router will reboot after the Upgrading has been finished.

### 5.11.3 Factory Defaults

This page (shown in figure 5-41) allows you to restore the factory default settings for the router.

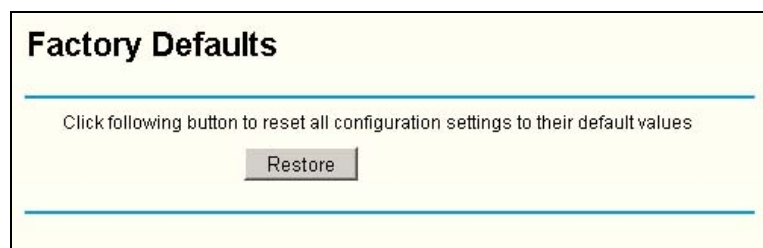


Figure 5-41: Restore Factory Default

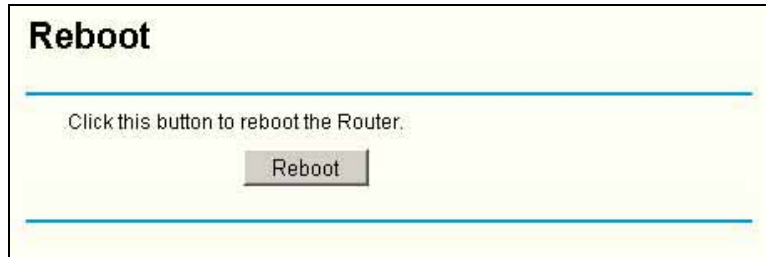
Click the **Restore** button to reset all configuration settings to their default values.

- The default **User Name**: admin
- The default **Password**: admin
- The default **IP Address**: 192.168.1.1
- The default **Subnet Mask**: 255.255.255.0

**Note:** Any settings you have saved will be lost when the default settings are restored.

### 5.11.4 Reboot

This page (shown in figure 5-42) allows you to reboot the router.

The image shows a web interface titled "Reboot". Below the title, there is a horizontal line. Underneath the line, the text "Click this button to reboot the Router." is displayed. Below this text is a single button labeled "Reboot". Another horizontal line is positioned below the button.

**Reboot**

---

Click this button to reboot the Router.

Reboot

---

Figure 5-42: Reboot the router

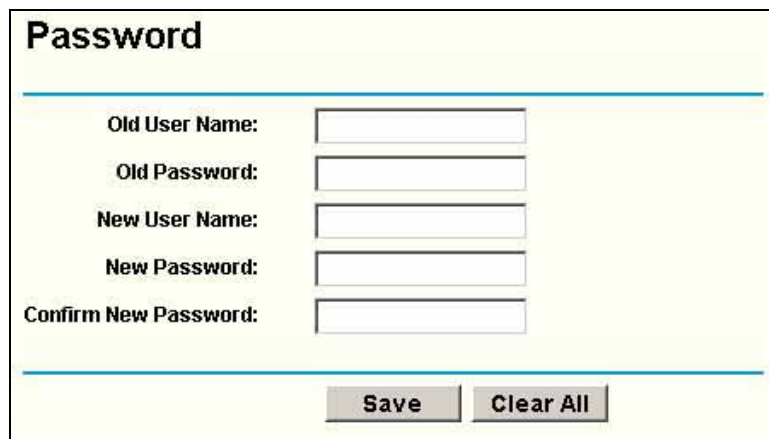
Click the **Reboot** button to reboot the router.

Some settings of the router will take effect only after rebooting, which include:

- Change LAN IP Address. (System will reboot automatically)
- MAC Clone (system will reboot automatically)
- DHCP service function.
- Static address assignment of DHCP server.
- Web Service Port of the router.
- Upgrade the firmware of the router (system will reboot automatically).
- Restore the router's settings to factory default (system will reboot automatically).

#### 5.11.5 Password

This page (shown in figure 5-43) allows you to change the factory default user name and password of the router.

The image shows a web interface titled "Password". Below the title, there is a horizontal line. Underneath the line, there are five labels with corresponding input fields: "Old User Name:", "Old Password:", "New User Name:", "New Password:", and "Confirm New Password:". At the bottom of the form, there are two buttons: "Save" and "Clear All".

**Password**

---

Old User Name:

Old Password:

New User Name:

New Password:

Confirm New Password:

---

Save Clear All

Figure 5-43: Password

It is strongly recommended that you change the factory default user name and password of the router. All users who try to access the router's web-based utility or Quick Setup will be prompted for the router's user name and password.

**Note:** The new user name and password must not exceed 14 characters in length and must not include any spaces. Enter the new Password twice to confirm it.

Click the **Save** button when finished.

Click the **Clear All** button to clear all.

### 5.11.6 Log

This page (shown in figure 5-44) allows you to query the Logs of the router.

**Log**

Index	Log
1	0000:System: Router initialization succeeded.

Time = 2003-05-01 8:12:11 731s  
H-Ver = WR641Gv2 00000000 : S-Ver = 1.0.6 Build 050530 Rel.31707n  
L = 192.168.1.1 : M = 255.255.255.0  
Mode = PPPoE : W = 0.0.0.0 : M = 0.0.0.0 : G = 0.0.0.0  
Free=6098, Busy=5, Bind=0, Inv=0/0, Bc=0/7, Dns=0, cl=91, fc=0/0, sq=0/0

RefreshClear Log

Figure 5-44: System Log

The router can keep logs of all traffic. You can query the logs to find what happened to the router.

Click the **Refresh** button to refresh the logs.

Click the **Clear Log** button to clear all the logs.

### 5.11.7 Statistics

The Statistics page (shown in figure 5-45) displays the network traffic of each PC on LAN, including total traffic and traffic of the last **Packets Statistic interval** seconds.

**Statistics**

Current Statistics Status: Disabled

Enable

Packets Statistics Interval(5-60): 5

Seconds

Save

☒ Auto-refresh

Refresh

Sorted Rules:

Sorted by Current Bytes

	Total		Current				
IP Address	Packets	Bytes	Packets	Bytes	ICMP Tx	UDP Tx	TCP SYN Tx
192.168.1.234	863	143559	19	3129	0/0	0/0	2/16

Figure 5-45: Statistics

- **Current Statistics Status** - Enable or Disable. The default value is disabled. To enable, click the **Enable** button. If disabled, the function of DoS protection in Security settings will be ineffective.
- **Packets Statistics Interval** - The default value is 10. Select a value between 5 and 60 seconds in the pull-down list. The Packets Statistic interval value indicates the time section of the packets statistic.
- **Sorted Rules** - here displays sort as desired.

**Statistics Table:**

<b>IP Address</b>		The IP Address displayed with statistics
<b>Total</b>	<b>Packets</b>	The total amount of packets received and transmitted by the router.
	<b>Bytes</b>	The total amount of bytes received and transmitted by the router.
<b>Current</b>	<b>Packets</b>	The total amount of packets received and transmitted in the last <b>Packets Statistic interval</b> seconds.
	<b>Bytes</b>	The total amount of bytes received and transmitted in the last <b>Packets Statistic interval</b> seconds.
	<b>ICMP Tx</b>	The total amount of the ICMP packets transmitted to WAN in the last <b>Packets Statistic interval</b> seconds.
	<b>UDP Tx</b>	The total amount of the UDP packets transmitted to WAN in the last <b>Packets Statistic interval</b> seconds.
	<b>TCP SYN Tx</b>	The total amount of the TCP SYN packets transmitted to WAN in the last <b>Packets Statistic interval</b> seconds.

Click the **Save** button to save the **Packets Statistic interval** value.

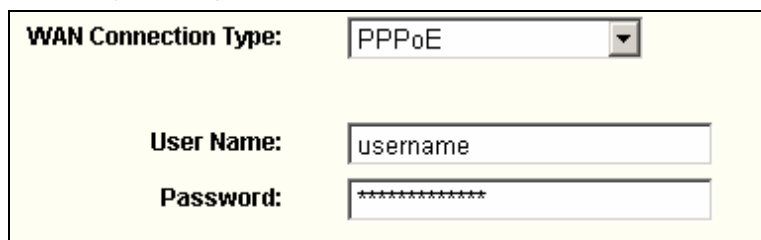
Click the **Auto-refresh** checkbox to refresh automatically.

Click the **Refresh** button to refresh immediately.

## Appendix A: FAQ

### 1. How do I configure the router to access Internet by ADSL users?

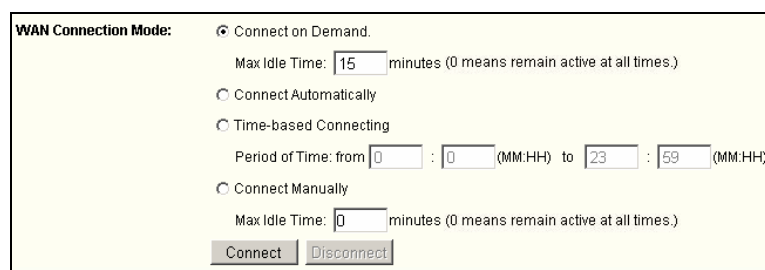
- 1) First, configure the ADSL modem configured in RFC1483 bridge model.
- 2) Connect the Ethernet cable from your ADSL modem to the WAN port on the router. The telephone cord plugs into the Line port of the ADSL modem.
- 3) Login to the router, click the "Network" menu on the left of your browser, and click "WAN" submenu. On the WAN page, select "PPPoE" for WAN Connection Type. Type user name in the "User Name" field and password in the "Password" field, finish by clicking "Connect".



The screenshot shows a web interface for configuring the WAN connection. The "WAN Connection Type:" dropdown menu is set to "PPPoE". Below it, the "User Name:" field contains the text "username", and the "Password:" field contains a series of asterisks "\*\*\*\*\*".

Figure A-1 PPPoE Connection Type

- 4) If your ADSL lease is in "pay-according-time" mode, select "Connect on Demand" or "connect Manually" for Internet connection mode. Type an appropriate number for "Max Idle Time" to avoid wasting paid time. Otherwise, you can select "Auto-connecting" for Internet connection mode.



The screenshot shows the "WAN Connection Mode:" section. The "Connect on Demand" radio button is selected. Below it, the "Max Idle Time:" is set to "15" minutes. There are also options for "Connect Automatically", "Time-based Connecting" (with a period of time from 00:00 to 23:59), and "Connect Manually" (with a "Max Idle Time:" of 0 minutes). At the bottom, there are "Connect" and "Disconnect" buttons.

Figure A-2 PPPoE Connection Mode

#### Note:

- i. Sometimes the connection cannot be disconnected although you specify a time to Max Idle Time, since some applications is visiting the Internet continually in the background.
- ii. If you are a Cable user, please configure the router following the above steps.

### 2. How do I configure the router to access Internet by Ethernet users?

- 1) Login to the router, click the "Network" menu on the left of your browser, and click "WAN" submenu. On the WAN page, select "Dynamic IP" for "WAN Connection Type", finish by clicking "Save".
- 2) Some ISPs require that you register the MAC Address of your adapter, which is connected to your cable or DSL modem during installation. If your ISP requires

MAC register, login to the router and click the "Network" menu link on the left of your browser, and then click "MAC Clone" submenu link. On the "MAC Clone" page, if your PC's MAC address is proper MAC address, click the "Clone MAC Address" button and your PC's MAC address will fill in the "WAN MAC Address" field. Or else, type the MAC Address into the " WAN MAC Address" field. The format for the MAC Address is XX-XX-XX-XX-XX-XX. Then click the "Save" button. It will take effect after rebooting.

Figure A-3 MAC Clone

### 3. I want to use Netmeeting, what do I need to do?

- 1) If you start Netmeeting as a sponsor, you don't need to do anything with the router.
- 2) If you start as a responsor, you need configure Virtual Server or DMZ Host.
- 3) How to configure Virtual Server: Login to the router, click the "Forwarding" menu on the left of your browser, and click " Virtual Servers" submenu. On the "Virtual Server" page, enter "1720" into the blank below the "Service Port", and your IP address below the IP Address, assuming 192.168.1.169 for an example, remember to "Enable" and "Save".

ID	Service Port	IP Address	Protocol	Enable
1	1720	192.168.1.169	ALL	<input checked="" type="checkbox"/>
2		192.168.1.	ALL	<input type="checkbox"/>
3		192.168.1.	ALL	<input type="checkbox"/>
4		192.168.1.	ALL	<input type="checkbox"/>

Common Service Port: DNS(53) Copy to ID 1

Previous Next Clear All Save

Figure A-4 Virtual Server

**Note:** Your opposite side should call your WAN IP, which is displayed on the "Status" page.

- 4) How to enable DMZ Host: Login to the router, click the "Forwarding" menu on the left of your browser, and click " DMZ" submenu. On the "DMZ" page, click "Enable" radio and type your IP address into the "DMZ Host IP Address" field, using 192.168.1.169 as an example, remember to click the "Save" button.

**DMZ**

☒ Enable ☐ Disable

DMZ Host IP Address: 192.168.1.169

Save

Figure A-5 DMZ

**4. I want to build a WEB Server on the LAN, what should I do?**

- 1) Because the WEB Server port 80 will interfere with the WEB management port 80 on the router, you must change the WEB management port number to avoid interference.
- 2) To change the WEB management port number: Login to the router, click the "Security" menu on the left of your browser, and click "Remote Management" submenu. On the "Remote Management" page, type a port number except 80, such as 88, into the "Web Management Port" field. Click "Save" and reboot the router.

**Remote Management**

Web Management Port: 88

Remote Management IP Address: 0.0.0.0

Save

Figure A-6 Remote Management

**Note:** If the above configuration takes effect, to configure to the router by typing <http://192.168.1.1:88> (the router's LAN IP address: Web Management Port) in the address field of the web browser.

- 3) Login to the router, click the "Forwarding" menu on the left of your browser, and click the "Virtual Servers" submenu. On the "Virtual Server" page, enter "80" into the blank below the "Service Port", and your IP address below the IP Address, assuming 192.168.1.188 for an example, remember to "Enable" and "Save".



### Virtual Servers

ID	Service Port	IP Address	Protocol	Enable
1	80	192.168.1.188	ALL	<input checked="" type="checkbox"/>
2		192.168.1.	ALL	<input type="checkbox"/>
3		192.168.1.	ALL	<input type="checkbox"/>
4		192.168.1.	ALL	<input type="checkbox"/>

Common Service Port:
DNS(53)
Copy to
ID
1

Previous
Next
Clear All
Save

Figure A-7 Virtual Server

**5. The wireless stations cannot connect to the router.**

- 1) Make sure the "Wireless Router Radio" is enabled.
- 2) Make sure that the wireless stations' SSID accord with the router's SSID.
- 3) Make sure the wireless stations have right KEY for encryption when the router is encrypted.
- 4) If the wireless connection is ready, but you can't access the router, check the IP Address of your wireless stations.

## Appendix B: Configuring the PCs

In this section, we'll introduce how to install and configure the TCP/IP correctly in Windows 95/98. First make sure your Ethernet Adapter is working, refer to the adapter's manual if needed.

### 1. Install TCP/IP component

- 1) On the Windows taskbar, click the **Start** button, point to **Settings**, and then click **Control Panel**.
- 2) Double-click the **Network** icon, click on the **Configuration** tab in the appearing **Network** window.
- 3) Click on the **Add** button. Select **Protocol**, and then click **Add**.

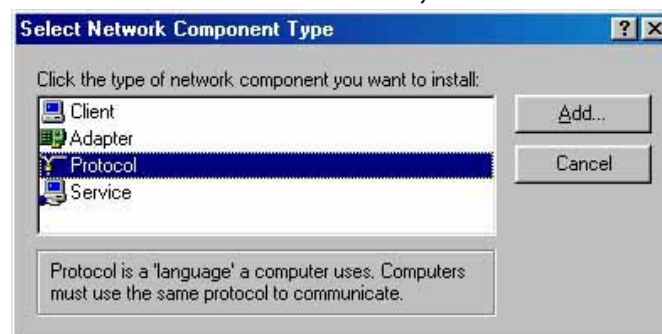


Figure B-1: Add Network Protocol

- 4) Under **Manufacturers** on **Select Network Protocol** page, highlight **Microsoft**. Under **Network Protocols**, highlight **TCP/IP**. Click **OK**. **TCP/IP** protocol will take effect after reboot.

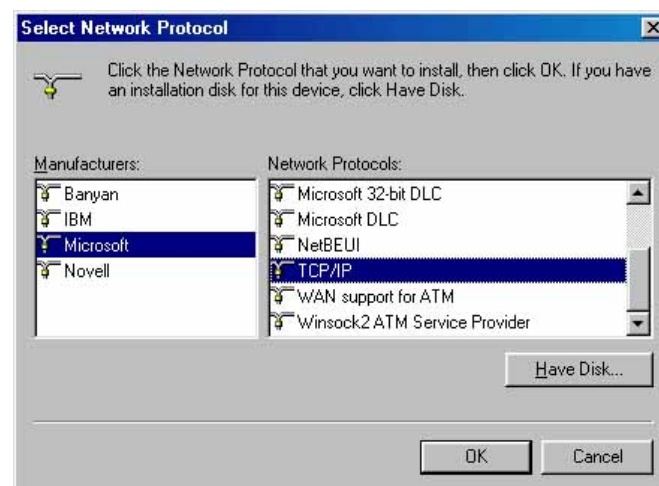


Figure B-2: Select Network Protocol

### 2. Configure TCP/IP for your computer

- 1) On the Windows taskbar, click the **Start** button, point to **Settings**, and then click **Control Panel**.
- 2) Double-click the **Network** icon, highlight the bound **TCP/IP** tab in the appearing **Network** window that appears. An example shown in the following figure:

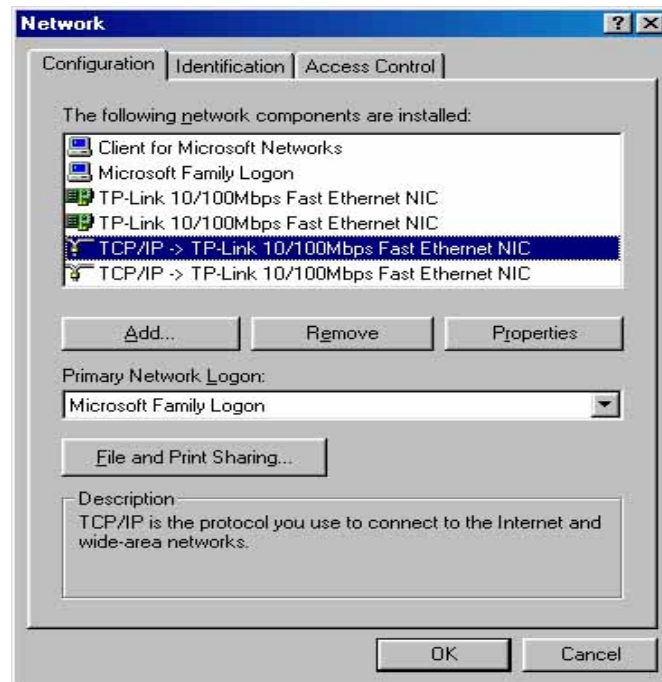


Figure B-3: Configuration tab

- 3) Click on **Properties**. The following **TCP/IP Properties** window will display and the **IP Address** tab is open on this window by default.
- 4) Now you have two ways to configure the **TCP/IP** protocol below:
  - **Assigned by DHCP Server**
    - a. Select **Obtain an IP address automatically**, as shown in the figure below:

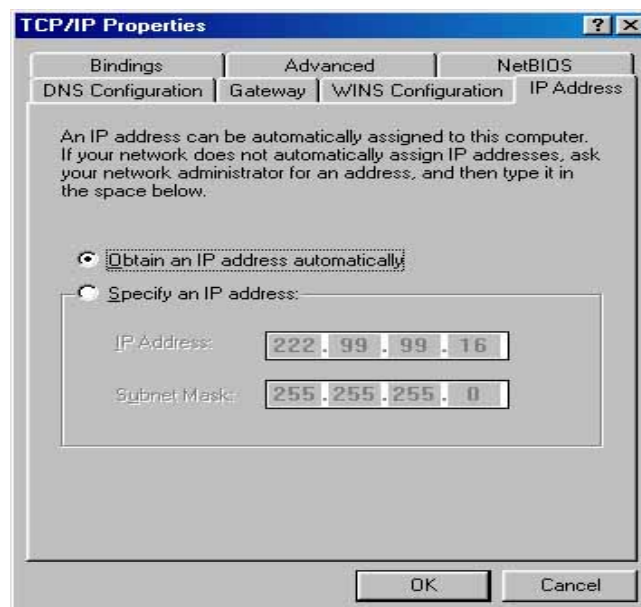


Figure B-4: IP Address tab

- b. Do not type anything into the **New gateway** field on the **Gateway** tab.



Figure B-5: Gateway tab

- c. Choose Disable DNS on the DNS configuration tab, as shown in the following figure:

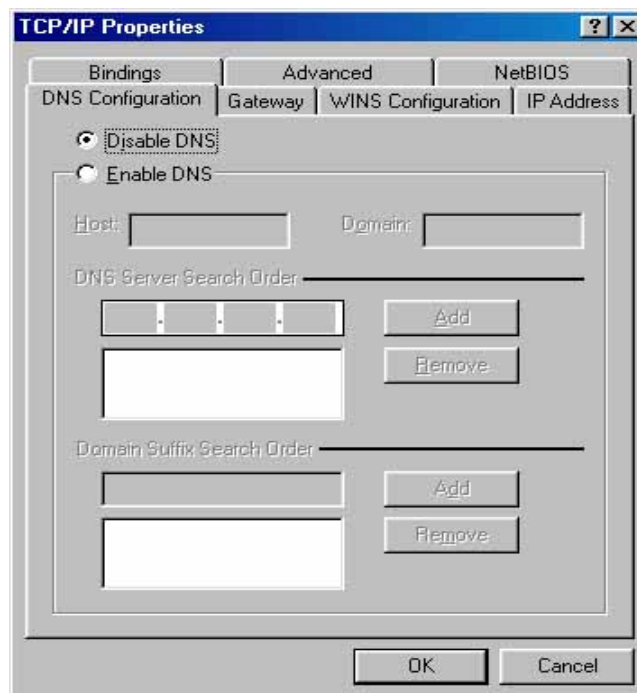


Figure B-6: DNS Configuration tab

- **Setting IP address manually**

- a. Select Specify an IP address on IP Address tab, as shown in the following figure. If the router's LAN IP address is 192.168.1.1, type IP address is 192.168.1.x (x is from 2 to 254), and subnet mask is 255.255.255.0.

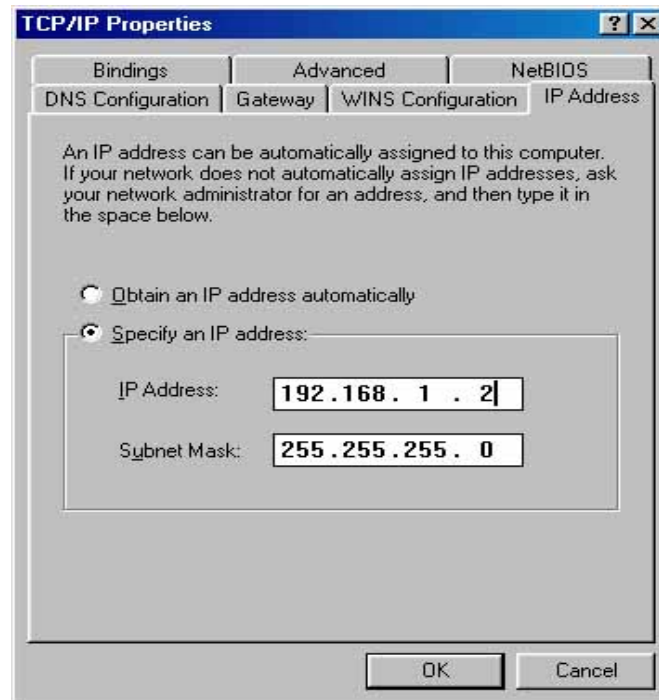


Figure B-7: IP Address tab

- b. Type the router's LAN IP address (the default IP is 192.168.1.1) into the **New gateway** field on the **Gateway** tab, and click on the **Add** button, as shown in the figure:

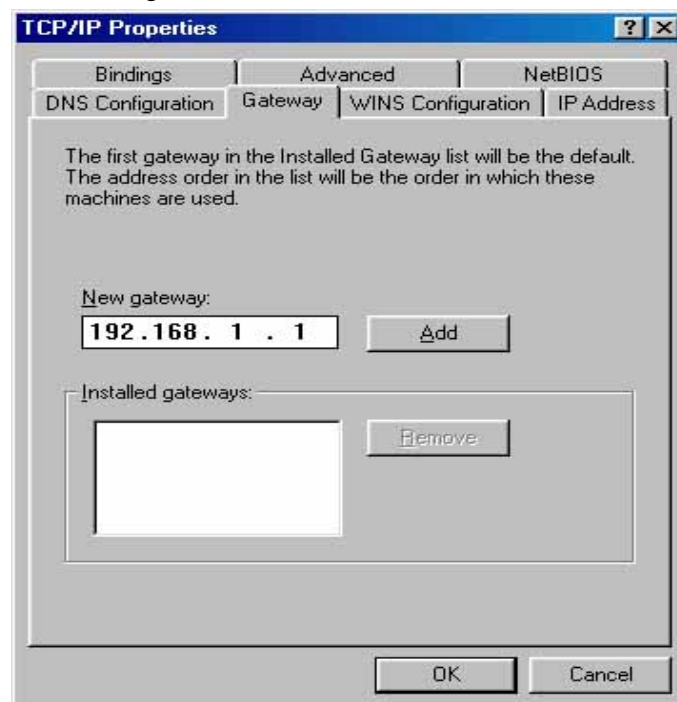


Figure B-8: Gateway tab

- c. On the **DNS Configuration** tab, click **Enable DNS** radio, and type your computer name in to the **Host** field and a Domain (such as szonline.com) into the **Domain** field. In the **DNS Server Search Order** field you can type the DNS server IP addresses, which has been provided by your ISP, and

click **Add** button. Shown below:

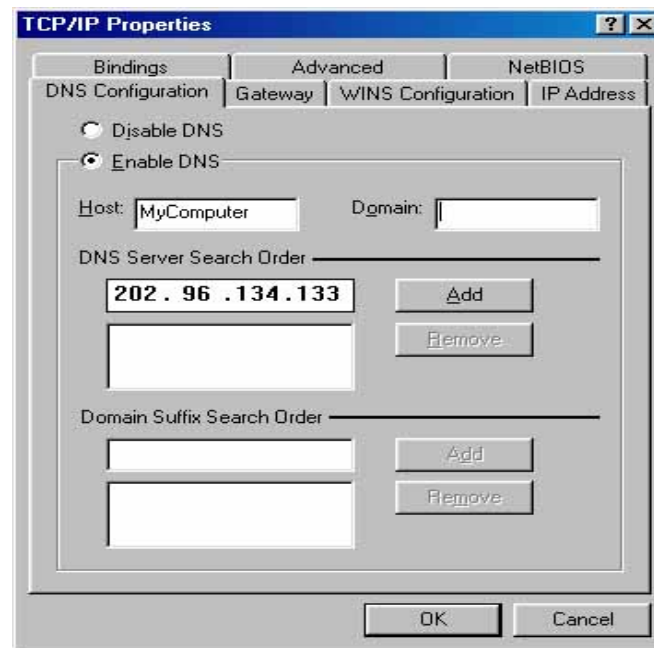


Figure B-9: DNS Configuration tab

**Now**, all the configurations are finished, it will take effect after reboot.

## Appendix C: Specifications

General	
Standards	IEEE 802.3, 802.3u, 802.11b and 802.11g
Protocols	TCP/IP, PPPoE, DHCP, ICMP, NAT, SNTP
Ports	One 10/100M Auto-Negotiation WAN RJ45 port, Four 10/100M Auto-Negotiation LAN RJ45 ports supporting Auto MDI/MDIX
Cabling Type	10BASE-T: UTP category 3, 4, 5 cable (maximum 100m) EIA/TIA-568 100Ω STP (maximum 100m) 100BASE-TX: UTP category 5, 5e cable (maximum 100m) EIA/TIA-568 100Ω STP (maximum 100m)
Radio Data Rate	108/54/48/36/24/18/12/9/6Mbps or 11/5.5/3/2/1Mbps
Power Supply	9V~ 0.8A
LEDs	Power, System, WLAN, Link/Act
Safety & Emissions	CE

## Appendix D: Glossary

- **108M Super G™ WLAN Transmission Technology** - 108M Super G™ WLAN Transmission Technology employs multiple performance-enhancing techniques including packet bursting, fast frames, data compression, and dynamic turbo mode that combine to improve the throughput and range of wireless networking products. Users can experience link rates of up to 108Mbps, twice the industry-standard maximum data link rate of 54Mbps, while preserving full compatibility with traditional 802.11g or 802.11b networks. 108M Super G™ products offer the highest throughput performance available on the market today. In dynamic 108M mode, the device can attach 802.11b, 802.11g and 108Mbps Super G™ devices at the same time in an integrated environment.
- **2x to 3x eXtended Range™ WLAN Transmission Technology** - The WLAN device with 2x to 3x eXtended Range™ WLAN transmission technology make its sensitivity up to 105 dB, which gives users the ability to have robust, longer-range wireless connections. With this range-enhancing technology, a 2x to 3x eXtended Range™ based client and access point can maintain a connection at as much as three times the transmission distance of traditional 802.11b and 802.11g products, for a coverage area that is up to nine times greater. A traditional 802.11b and 802.11g product transmission distance is about 300m, A 2x to 3x eXtended Range™ based client and access point can maintain a connection transmission distance may be up to 830m.
- **802.11b** - The 802.11b standard specifies a wireless networking at 11 Mbps using direct-sequence spread-spectrum (DSSS) technology and operating in the unlicensed radio spectrum at 2.4GHz, and WEP encryption for security. 802.11b networks are also referred to as Wi-Fi networks.
- **802.11g** - specification for wireless networking at 54 Mbps using direct-sequence spread-spectrum (DSSS) technology, using OFDM modulation and operating in the unlicensed radio spectrum at 2.4GHz, and backward compatibility with IEEE 802.11b devices, and WEP encryption for security.
- **DDNS (Dynamic Domain Name System)** - The capability of assigning a fixed host and domain name to a dynamic Internet IP Address.
- **DHCP (Dynamic Host Configuration Protocol)** - A protocol that automatically configure the TCP/IP parameters for the all the PCs that are connected to a DHCP server.
- **DMZ (Demilitarized Zone)** - A Demilitarized Zone allows one local host to be exposed to the Internet for a special-purpose service such as Internet gaming or videoconferencing.
- **DNS (Domain Name System)** – An Internet Service that translates the names of websites into IP addresses.



- **Domain Name** - A descriptive name for an address or group of addresses on the Internet.
- **DoS (Denial of Service)** - A hacker attack designed to prevent your computer or network from operating or communicating.
- **DSL (Digital Subscriber Line)** - A technology that allows data to be sent or received over existing traditional phone lines.
- **ISP (Internet Service Provider)** - A company that provides access to the Internet.
- **MTU (Maximum Transmission Unit)** - The size in bytes of the largest packet that can be transmitted.
- **NAT (Network Address Translation)** - NAT technology translates IP addresses of a local area network to a different IP address for the Internet.
- **PPPoE (Point to Point Protocol over Ethernet)** - PPPoE is a protocol for connecting remote hosts to the Internet over an always-on connection by simulating a dial-up connection.
- **SSID - A Service Set Identification** is a thirty-two character (maximum) alphanumeric key identifying a wireless local area network. For the wireless devices in a network to communicate with each other, all devices must be configured with the same SSID. This is typically the configuration parameter for a wireless PC card. It corresponds to the ESSID in the wireless Access Point and to the wireless network name.
- **WEP (Wired Equivalent Privacy)** - A data privacy mechanism based on a 64-bit or 128-bit or 152-bit shared key algorithm, as described in the IEEE 802.11 standard.
- **Wi-Fi** - A trade name for the 802.11b wireless networking standard, given by the Wireless Ethernet Compatibility Alliance (WECA, see <http://www.wi-fi.net>), an industry standards group promoting interoperability among 802.11b devices.
- **WLAN (Wireless Local Area Network)** - A group of computers and associated devices communicate with each other wirelessly, which network serving users are limited in a local area.